



**ВЕСТНИКЪ КРИМИНАЛИСТИКИ
BULLETIN OF CRIMINALISTICS**

I (77) - 2021

Издается с 1999 г.

*Основатель журнала и его первый ответственный редактор
профессор А.Т. Филиппов*

Ответственный редактор Е.В. Иванова

В журнале

«ВЕСТНИКЪ КРИМИНАЛИСТИКИ ~ BULLETIN OF CRIMINALISTICS»

*публикуются статьи по криминалистике, судебной экспертизе, оперативно-
розыскной деятельности, представляющие интерес для практикующих
работников правоохранительных органов, а также адвокатов, судей,
преподавателей и научных работников.*

ISSN 2220-847X

Адрес редакции:

author@vestcrim.ru, contact@fact-gsgu.ru

2021





Редакционная коллегия:

Главный редактор: *Иванова Елена Вячеславовна, доктор юридических наук, доцент (Государственный социально-гуманитарный университет).*

Заместитель главного редактора: *Дьяконова Оксана Геннадьевна, кандидат юридических наук, доцент (Московский государственный юридический университет имени О.Е. Кутафина).*

Редакционный совет:

Аубакирова Анна Александровна, доктор юридических наук, доцент (Алматинская академия МВД Республики Казахстан имени М. Есбулатова);

Белкин Анатолий Рафаилович, кандидат физико-математических наук, доктор юридических наук, профессор (Российский технологический университет);

Бошкovich Александр, доктор юридических наук (PhD), адъюнкт-профессор уголовного процессуального права, The Academy of Criminalistic and Police Studies in Belgrade, the Republic of Serbia.

Гармаев Юрий Петрович, доктор юридических наук, профессор (Кубанский государственный аграрный университет)

Трибунов Олег Павлович, доктор юридических наук, доцент (Восточно-Сибирский институт МВД России);

Зайцева Елена Александровна, доктор юридических наук, профессор (Волгоградская академия МВД России);

Зинин Александр Михайлович, доктор юридических наук, профессор, (Московский государственный юридический университет имени О. Е. Кутафина);

Matulienė Snieguolė, PhD, (Mūsų Romerio universitetas, Vilnius, Литва);

Майлис Надежда Павловна, доктор юридических наук, профессор (Московский университет МВД России имени В.Я. Кикотя);

Моисеева Татьяна Федоровна, доктор юридических наук, профессор (Российский государственный университет правосудия);

Россинская Елена Рафаиловна, доктор юридических наук, профессор (Институт судебных экспертиз Московского государственного юридического университета имени О. Е. Кутафина);

Филиппов Александр Георгиевич, кандидат юридических наук, профессор (Московский университет МВД России).

Ялышев Станислав Алимович, доктор юридических наук, профессор (Российский государственный университет правосудия).





ВЕСТНИКЪ КРИМИНАЛИСТИКИ
BULLETIN OF CRIMINALISTICS
I (77) - 2021

Published since 1999

The founder of the journal and first Executive editor

Professor A. G. Filippov

Executive editor

Doctor of Law Sciences, docent E.V. Ivanova

The journal

«ВЕСТНИКЪ КРИМИНАЛИСТИКИ ~ BULLETIN OF CRIMINALISTICS»

*Published articles on criminalistics, forensic examination, operational
investigative activity of interest to practitioners law enforcement agencies, as
well as lawyers, judges, teachers and scientific workers*

ISSN 2220-847X

2021



СОДЕРЖАНИЕ

От главного редактора	5
-----------------------------	---

ПРОТИВОДЕЙСТВИЕ ИНФОРМАЦИОННО-МИРОВОЗЗРЕНЧЕСКИМ УГРОЗАМ В ИНТЕРНЕТ-СРЕДЕ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНЫХ ЗНАНИЙ

БЕРЕЖНАЯ Д.А. Художественный или квазихудожественный текст: к разработке экспертной технологии исследования информационных материалов в рамках противодействия экстремизму	6
--	---

ВЕНЦЕЛЬ С.В. Формирование критического мышления как инструмента противодействия экстремизму в эпоху новых медиа.....	13
--	----

ГОРБУНОВА Е.Ю., ХОМИН Д.М. Актуальные проблемы использование специальных знаний в области компьютерной техники и программного обеспечения при расследовании мошенничеств, совершенных с использованием вредоносных программ.....	19
--	----

ДОРОФЕЕВ К.И. Проблемные аспекты использования специальных знаний при расследовании изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних	35
--	----

ДОРОШЕНКО Е.И. Стратегические коммуникации в противодействии идеологии экстремизма и терроризма в эру коронавируса и «пост-правды».....	42
---	----

КАРЕПАНОВ Н.В. Некоторые проблемы криминалистического выявления и исследования вредоносных компьютерных программ.....	48
---	----

ЛЕБЕДЕВА А.К. О пропаганде наркотических средств в сети Интернет в аспекте судебной лингвистической экспертизы	57
--	----

МЫСКИНА К.М. Соблюдение конфиденциальности информации как принцип судебно-экспертной этики.....	63
---	----

САРКИСЯН А.А. Информационная безопасность экспертных учреждений в эпоху цифровизации.....	69
---	----

ТРОИЦКАЯ Т.А. Использование нетрадиционных для судебно-экспертной практики научных дисциплин для исследования материалов с порнографическим или оскорбительным контентом, размещенных в сети Интернет, как способ объективизации результатов экспертной деятельности	74
--	----

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИКИ И СУДЕБНОЙ ЭКСПЕРТИЗЫ

АБРАМОВА А.А., КУЧИН О.С. Виды экспертиз, проводимых при расследовании финансирования терроризма	81
--	----

ГРИГОРОВИЧ В.Л. О понятии и предмете криминалистической одорологии	90
--	----

КРИМИНАЛИСТИКА И СУДЕБНАЯ ЭКСПЕРТИЗА ЗА РУБЕЖОМ

ХОЛЕВЧУК А.Г., УВАРОВ А.В. Проблемы одорологической детекции запаховых следов каннабиса: опыт США	97
---	----

НАУЧНАЯ ЖИЗНЬ

Международная научно-практическая конференция «Теория и практика судебной экспертизы в современных условиях»	106
--	-----

ТРЕБОВАНИЯ ДЛЯ АВТОРОВ	118
------------------------------	-----

ОТ ГЛАВНОГО РЕДАКТОРА

Уважаемые читатели!

3 декабря 2020 года кафедрой судебных экспертиз Университета имени О. Е. Кутафина (МГЮА) совместно с Российским федеральным центром судебной экспертизы при Министерстве юстиции РФ и Центром академического развития и образовательных инноваций МГЮА была проведена научно-практическая конференция с международным участием в онлайн-режиме на тему «Противодействие информационно-мировоззренческим угрозам в интернет-среде с использованием специальных знаний». На конференции были представлены доклады по общетеоретическим и прикладным проблемам криминалистического и юридико-лингвистического обеспечения информационно-мировоззренческой безопасности в интернет-среде. Особое внимание организаторы уделили обсуждению дискуссионных вопросов использования специальных знаний для обеспечения информационно-мировоззренческой безопасности в интернет-медиа (противодействие экстремизму; буллинг; троллинг; пропаганде суицида, тюремной культуры, культа насилия и жестокости; секстингу; грумингу; фейкингу; диффамации и т.д.), а также криминалистическим проблемам использования специальных знаний при исследовании вредоносных компьютерных программ, контрафактной и недокументированной информационно-компьютерной продукции.

В представленном номере журнала «Вестник криминалистики» публикуем некоторые из представленных на конференции докладов¹.

¹ Статьи публикуются в авторской редакции.

ПРОТИВОДЕЙСТВИЕ ИНФОРМАЦИОННО-МИРОВОЗРЕНЧЕСКИМ УГРОЗАМ В ИНТЕРНЕТ-СРЕДЕ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНЫХ ЗНАНИЙ

ХУДОЖЕСТВЕННЫЙ ИЛИ КВАЗИХУДОЖЕСТВЕННЫЙ ТЕКСТ: К РАЗРАБОТКЕ ЭКСПЕРТНОЙ ТЕХНОЛОГИИ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННЫХ МАТЕРИАЛОВ В РАМКАХ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ

БЕРЕЖНАЯ Д.А.

Рассматриваются вопросы экспертного психологического исследования художественных текстов по делам, связанным с противодействием экстремизму, проблема достаточности экспертных понятий в данной экспертной области, обусловленная спецификой объекта исследования, анализа художественной коммуникации. Предложены некоторые элементы технологии различения художественного и квазихудожественного текста как метазадачи исследования информационных материалов художественного типа на предмет установления специальных признаков экстремистских значений.

Ключевые слова: судебная психологическая экспертиза, психолого-лингвистическая экспертиза, судебная экспертология, произведение искусства, художественное произведение, литературное произведение, квазихудожественное произведение, психология искусства, экстремизм.

Информационные материалы художественного типа подлежат оценке в рамках экспертной деятельности по противодействию и профилактике экстремизма [4, 5, 10, 11]. Однако практика показывает, что существует необходимость разработки особого варианта технологии исследования художественного (или представленного как таковой) текста, особенно с учетом доминирования в современных реалиях спорных информационных материалов интернет-медиа, затрудняющего «опознание» материалов истинно художественного типа и эстетизированных, *квазихудожественных* элементов, встроенных в информационные продукты, обеспечивающие различного рода деструктивные социальные практики, в том числе экстремистскую деятельность.

Анализ художественной коммуникации и материалов художественного типа относится к категории повышенной сложности, что обусловлено комплексом факторов разнопорядкового и разнопланового характера. С одной стороны, факторы сложности, связанные с полимотивированностью художественной деятельности и коммуникации, с другой - факторы, связанные непосредственно с особенностями художественных текстов, – многозначностью и полиинтерпретативностью, стилистическими особенностями, «многослойностью» проявления в тексте автора (рассказчика, персонажа) и сложностью установления авторской позиции [4, 10, 11], многообразием средств выразительности и пр. Кроме того, сложность данной категории текстов для экспертной практики обусловлена также и методической (технологической) лакуной, что легко видеть на самых первых этапах

экспертного исследования – при исследовании коммуникативной ситуации, в которой функционирует исследуемый текст, а именно анализ таких *условий высказывания*, как использованные средства и тип коммуникации.

При этом междисциплинарный, комплексный подход к исследованию текстов (произведений), выраженных в художественной форме (даже исключительно словесной), ориентированный на исследование коммуникативных действий и коммуникативной деятельности [3] и установление социально-психологической направленности объекта исследования, а не оценку самих по себе словесных и/или изобразительных материалов, обосновано являющийся актуальным трендом в судебной экспертизе [12], представляется обязательным.

Важно, что анализ должен носить содержательно комплексный характер на каждом этапе исследования, что должно обеспечить отсутствие операциональных экспертных ошибок, предотвратить ситуацию невозможности реализовать синтезирующий анализ (и получить автономный анализ лингвиста и психолога). Имеющийся инструментарий комплексной психолого-лингвистической судебной экспертизы информационных материалов – Методика проведения комплексной судебной психолого-лингвистической экспертизы по делам, связанным с противодействием экстремизму и терроризму (далее – Методика) [6] в целом применим к данной категории текстов [11]. Авторы Методики формулируют требование оценить тип коммуникации по характеру отражения действительности, т. е. дифференцировать нехудожественную и художественную коммуникацию. Именно выполнение этой задачи и должно, с нашей точки зрения, определить дальнейшую логику комплексного анализа (степень развернутости соответствующих подвыводов в заключении эксперта обуславливается тем, что именно квалифицировано как художественный текст – смысловое целое или его элемент, например, фоновая песня в видеоролике, уточняющая и/или иллюстрирующая выраженные значения, но не формирующая самостоятельно социально-психологическую направленность всего объекта).

Различие этих двух типов коммуникации и, соответственно, методов анализа художественного и нехудожественного текста достаточно традиционно для научно-исследовательских целей. Предикативный анализ текста, предложенный Н. И. Жинкиным и его школой, информативно-целевой анализ Т. М. Дридзе имеют свою специфику для художественных текстов; точнее сказать, вводят ограничение на применение метода. См., например, у А. А. Леонтьева о невозможности сохранения смыслового тождества по центральным смысловым компонентам текста при его компрессии [7]. Безусловно, это различие необходимо учитывать и в практике судебной экспертизы, вырабатывать современные, частные технологии анализа медиа-текстов, позволяющие на языке экспертных (субэкспертных по уровню) понятий формулировать это различие для обеспечения полного и всестороннего исследования художественного текста на предмет наличия / отсутствия «экстремистских» значений.

Отправной точкой могла бы стать формулировка метазадачи, которую совместно решают эксперты лингвист и психолог при анализе информационных материалов художественного типа: оценка объекта как *художественного* текста (единство содержания и

БЕРЕЖНАЯ Д. А.

формы) или как *квази*художественного текста («превращенной», «трангрессированной» художественной формы – формы, не «сохраняющей» единства с содержанием, деконструированного в результате целенаправленной коммуникативной (включая речевую) деятельности автора/публикатора единства формы и содержания. В первом случае общая логика технологии экспертного анализа и представления результатов исследования в целом ясна и вряд ли может вызывать существенные затруднения: компоненты искомых значений, прежде всего целевой, исследуются в логике социальных функций искусства (познавательно-эвристической, художественно-концептуальной, воспитательной и иным [см., например 2, с.11-12], что проявляется в доминирующих интенциях привлечения внимания, интереса, порождения индивидуального отношения к проблемам действительности, «подвергнутым» осмыслению автором; установление эмоционального контакта с реципиентом и др. под.), результаты формулируются на языке анализа художественного произведения. В этом случае, следует отметить, технология должна разрабатываться преимущественно «на стороне» эксперта-психолога (эксперты-лингвисты в методическом аспекте готовы к применению такого анализа существенно лучше).

При решении метазадачи оценки текста как художественного или *квази*художественного в фокусе внимания должны быть следующие реперные точки:

- трехчастная коммуникативная структура автор – произведение – реципиент; разграничение *конфликта* как свойства текста (как с точки зрения смысловой структуры, так и с точки зрения потенциала воздействия на реципиента) и как объекта отображения (предметно-тематический компонент диагностических комплексов в Методике);

- особенности экспрессивной коммуникации, такие как особая позиция (обусловленная доминирующей интенцией на создание общественно-значимого высказывания / произведения и опосредованному [произведением] эмоциональному контакту с адресатом) автора текста, эмоциональная вовлеченность автора-творца (что *не* идентично выразительности текста, подвывод психологического исследования не может механически опираться на соответствующие результаты лингвистического анализа), и как следствие особые «требования» к художественной компетентности реципиента (оценочный компонент диагностических комплексов в Методике). Психологические средства воплощения смыслов в структуре художественного произведения, которые могут быть исследованы на данном этапе, например хроника, хронотопика, метафорика, символика, семантика, архетипика, архитектурика; при этом «носителями смыслов все перечисленные структуры выступают лишь в отношении к конкретному воплощенному в них содержанию, вне которого они лишены какого бы то ни было смыслового содержания» [2, с. 37]. Отметим, что краткий анализ «технической» стороны художественного текста необходим прежде всего для аргументации целенаправленности коммуникативной деятельности автора и ее характеристики с точки зрения присутствия в структуре произведения названных выше средств реализации «задачи на смысл» (в терминологии Д. А. Леонтьева). Однако, природа художественного текста не сводима к богатству технических приемов («нахождение технических приемов художественного творчества, способов организации художественного текста не может открыть тайны эмоционального воздействия произведений искусства. Использование тех или иных художественных приемов еще не создает художественного текста, не они определяют художественность произведения» [1, с. 32]). Очевидно, что их

обнаружение не являются целью психологического анализа информационных материалов в рамках противодействия экстремизму и терроризму; а суждения об их отсутствии или недостаточной выраженности как аргумента в пользу наличия специальных признаков «экстремистских» значений, обоснование наличия таких признаков через указание на отсутствие художественной, идейной ценности, примитивности, грубости, «сниженности» использованных средств и т.п. – недопустимо;

– различение функциональной и содержательной, социально-психологической направленности текста; различение вовлечения реципиента в опосредованный эмоциональный контакт как *цели* или *средства*; и в конечном итоге – направленности на формирование готовности к индивидуальной эстетической (в широком смысле, без сведения к «катарсическим» или реакциям «эстетического наслаждения») реакции на художественный текст (в том числе социально-психологических художественных установок (иначе установок на искусство) различных типов, установки к развитию художественной компетентности, экспертности восприятия художественных текстов [2, 8, 9]) в противовес направленности на формирование «экстремистских» установок. Последнему – *квазихудожественному* «экстремистскому» тексту безусловно может быть придан эстетический слой, что мы и назвали условно «превращенной», «трангрессированной» формой, в том числе как средство достижения основной коммуникативной направленности деятельности автора (целевой компонент диагностических комплексов в Методике). Оговоримся здесь, что философский термин «превращенная форма» занят, мы используем его как указатель на общую идею, стимульное образное выражение для поиска корректного психологического экспертного понятия.

Критерии оценки текста как художественного представляют сами по себе исследовательскую проблему, не решенную в психологической науке. Вопрос решается и «от автора», и «от произведения», и «от реципиента» [8, 9]. Операционализировать их в экспертных понятиях довольно сложная задача. Приведем в пример критерий, предложенный В. М. Аллахвердовым: «Если текст порождает такие осознанные и неосознанные противоречия, что решение осознанных противоречий приводит к нарушению неосознанных, то данный текст является художественным текстом» [1, 59].

Казалось бы, естественный методический ход – обратиться непосредственно к понятиям философии и эстетики для построения психологии искусства, показывает, что его нельзя считать достаточным. Проиллюстрируем мысль словами В. М. Аллахвердова, подытоживающими дискуссию о предложенной им гипотезе о природе эмоционального воздействия искусства: «Я согласен и с тем, что было, наверное, правильно ввести в объяснительные конструкции термины, принятые в эстетике: «художественный образ»..., «гармония»..., «сотворчество»... и другие. Но – трудность – эти слова плохо определены...» [1, с. 197]. Соответственно, следующий шаг – формирование экспертных понятий с опорой на развитые психологические теории и модели порождения и восприятия искусства, художественного творчества – оказывается тем более затруднительным и, как минимум представляет самостоятельную задачу для разработки экспертной технологии психологического исследования информационных материалов. Подчеркнем, терминология теории искусства (искусствознания) и эстетики, относящаяся к «хорошему» (или «плохому»,

БЕРЕЖНАЯ Д. А.

что вероятнее в экспертной практике) художественному тексту, не пригодна для анализа текстов в контексте противодействия экстремизму; ее наличие в тексте заключения эксперта психолога (позволим себе - и лингвиста) в качестве опорной для характеристики исследуемого текста само по себе является основанием для крайне осторожного отношения к полученным выводам.

Важно, что экспертная ошибка (или небрежность при представлении результатов исследования, что фактически должно быть расценено как ошибка), прозрачно и недвусмысленно не снимающая жестко *альтернативных* вариантов интерпретации текста как *художественного* или *квазихудожественного* (последовательно сформулированной на уровне соответствующего «субэкспертного языка» от компонента к компоненту диагностических комплексов Методики), допускающая смешение эксплицируемых смыслов текста в любом компоненте может привести к гносеологическим ошибкам.

Сложность информационных материалов художественного характера, связанная с комплексом указанных факторов нередко и является причиной того, что художественный текст становится спорным объектом в контексте противодействия и профилактики экстремистской деятельности, или квалифицируется как «экстремистский» – не только в восприятии граждан (приведем в пример случай исследования орнаментальных кованных перил, обрамляющих крыльцо магазина, на предмет установления признаков пропаганды идеологии нацизма), но и при первичной оценке сотрудниками правоохранительных органов. Такое положение дел может быть преодолено в русле уточнения и детализации имеющихся экспертных технологий: формирования теоретических предпосылок различения художественного и *квазихудожественного* текста, постановки мета- и субзадач, выработки соответствующих субэкспертных понятий.

Библиографический список:

1. Алахвердов В. М. Психология искусства. Эссе о тайне эмоционального воздействия художественных произведений. СПб.: ДНК, 2001. 200 с.
2. Крупник Е. П. Психологическое воздействие искусства. М.: ИП РАН, 1999. 240 с.
3. Кроз М. В., Ратинова Н. А. История и современное состояние экспертных исследований экстремистских материалов // Теория и практика судебной экспертизы. 2016. Том 43. № 3. С. 146-154.
4. Кузнецов С. А., Оленников С. М. Экспертные исследования по делам о признании информационных материалов экстремистскими: теоретические основания и методическое руководство (научно-практическое издание) / 2-е изд., испр. И доп. М.: Издательский дом В. Ема, 2014. 312 с.
5. Кукушкина О.В., Сафонова Ю.А., Секераж Т.Н. Теоретические и методические основы судебной психолого-лингвистической экспертизы текстов по делам, связанным с противодействием экстремизму. М.: РФЦСЭ, 2011. 331 с.
6. Кукушкина О.В., Сафонова Ю.А., Секераж Т.Н. Методика проведения комплексной судебной психолого-лингвистической экспертизы по делам, связанным с противодействием экстремизму и терроризму. М.: РФЦСЭ, 2014. 98 с.
7. Леонтьев А. А. Основы психолингвистики. М.: Смысл, 1999. 287 с.
8. Леонтьев Д. А. Введение в психологию искусства. М.: МГУ, 1998. 111 с.

9. Leontiev D. A. The Perception of Art: Psychological Mechanisms, Factors, and Processes // Journal of Russian and East European Psychology. vol. 38, no. 3. NY.: M.E. Sharpe 2000. Pp. 45–63.

10. Плотникова А. М. Лингвистическая экспертиза художественного текста по делам о противодействии экстремизму // Теория и практика судебной экспертизы. 2014. Том 36, № 4, С. 18-21.

11. Плотникова А. М. Конфликтная коммуникация в аспекте судебной лингвистики. Е М.: TXT, 2017. 197 с.

12. Смирнова С. А., Секераж Т. Н., Кузнецов В. О. Междисциплинарные исследования в судебно-экспертных учреждениях Минюста России: актуальные направления лингвистической и психологической экспертизы // Теория и практика судебной экспертизы. 2017. Том 12, № 4, С. 6-11.

13. Судебная экспертиза: типичные ошибки / Под ред. Е. Р. Россинской. М.: Проспект, 2018. 544 с.

References:

1. Allakhverdov V. M. Psychology of Art. Essay on the mystery of the emotional impact of works of art. St.P.: DNK. 2001. 200 p. (In Russ.)

2. Krupnik E.P. The psychological impact of art. M.: IP RAS, 1999. 240 p. (In Russ.)

3. Kroz M. V., Ratinova N. A. History and Current State of Forensic Analysis of Extremist Materials. Theory and Practice of Forensic Science. 2016. Vol. 43. No 3, P. 146-154. (In Russ.)

4. Kuznetsov S.A., Olennikov S.M. Ekspertnye issledovaniya po delam o priznanii informatsionnykh materialov ekstremistskimi: teoreticheskie osnovaniya i prakticheskoe rukovodstvo [Expert researches on cases of recognition of information materials extremist: theoretical bases and practice guidance]. 2nd edition. Moscow: V. Ema Publ., 2014. 312 p. (In Russ.)

5. Kukushkina O.V., Safonova Yu.A., Sekerazh T.N. Theoretical and methodical bases of forensic psychological and linguistic examination of texts on the affairs connected with counteraction to extremism. Moscow: RFCFS, 2011. 331 p. (In Russ.)

6. Kukushkina O.V., Safonova Yu.A., Sekerazh T.N. Method of conducting complex forensic psychological and linguistic examination of the affairs connected with counteraction to extremism and terrorism. Moscow: RFCFS, 2014. 98 p. (In Russ.)

7. Leontiev A. A. Basics of psycholinguistics. M.: Smysl, 1999. 287 p. (In Russ.)

8. Leontiev D. A. Introduction to Psychology of Art. M.: MSU, 1998. 111 p. (In Russ.)

9. Leontiev D. A. The Perception of Art: Psychological Mechanisms, Factors, and Processes // Journal of Russian and East European Psychology. vol. 38, no. 3. NY.: M.E. Sharpe 2000. Pp. 45–63.

10. Plotnikova A. M. Linguistic Assessment of Literary Texts in Cases Related to Extremism Prevention. Theory and Practice of Forensic Science. 2014. Vol. 36. No 4, P. 18-21. (In Russ.)

БЕРЕЖНАЯ Д. А.

11. Plotnikova A. M. Conflictual Communication In Forensic Linguistics. E M.: TXT, 2017. 197 p. (In Russ.)

12. Smirnova S.A., Sekerazh T.N., Kuznetsov V.O. Interdisciplinary Evaluations Performed by Forensic Science Organizations of the Russian Ministry of Justice: Current Trends in Forensic Linguistics and Forensic Psychology. Theory and Practice of Forensic Science. 2017. Vol. 12. No 4. P. 6–11. (In Russ.)

13. Rossinskaya E.R. (ed.) Forensic science: typical mistakes. M.: Prospekt, 2018. 544 p. (In Russ.)

Daria A. Berezhnaya

**ARTISTIC WORK VS QUASI-ARTISTIC WORK: TO THE TECHNOLOGY OF
INFORMATION MATERIALS ANALYSIS FOR COUNTERING EXTREMISM**

The article considers the issues of forensic psychological analysis of artistic type informational materials in cases related to countering extremism. The author examines the problem of expert terms for forensic expertology, primarily due to limitations of applying results from studies in areas such as psychology of art, aesthetics to legal questions, as well as the specifics of the forensic analysis of artistic communication and artistic work. The author describes some elements of the technology to find out special signs of “extremist” meanings in cases with artistic type informational materials. It is proposed to distinguish artistic and quasi-artistic works as meta-task of integral linguistic and psychological analysis.

Keywords: forensic psychological evaluation, integrated psychological and linguistic analysis / psycholinguistic analysis, forensic expertology, artwork, artistic work, literary work, quasi-artistic work, psychology of art, extremism.

Сведения об авторе:

Бережная Дарья Анатольевна, Институт общественных наук РАНХиГС, старший преподаватель кафедры общей психологии факультета психологии

Адрес электронной почты: d.berejnaya@gmail.com

About the author:

Daria A. Berezhnaya, Institute for Social Sciences of the Russian Presidential Academy of National Economy and Public Administration (RANEPA), Senior Lecturer at the Department General Psychology, Faculty of Psychology.

Email: d.berejnaya@gmail.com

ФОРМИРОВАНИЕ КРИТИЧЕСКОГО МЫШЛЕНИЯ КАК ИНСТРУМЕНТА ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В ЭПОХУ НОВЫХ МЕДИА

ВЕНЦЕЛЬ С.В.

Автор актуализирует проблему формирования критического мышления как действенного инструмента в противодействии процессам радикализации в эпоху становления новых медиа. В качестве цели автор ставит необходимость понимания структуры механизмов критического мышления для подчеркивания практической пользы в специфическом коммуникативном пространстве новых медиа. Автором подчеркиваются ключевые особенности новых медиа как пространства безграничного творчества всех пользователей. В то же время автором отмечается ряд актуальных теоретико-методологических сложностей в разрешении проблемы, а именно отсутствие единого подхода к пониманию сущности экстремизма и продолжающиеся научные дискуссии о сущности новых медиа. Автор приходит к выводу о том, что только комплексная система противодействия экстремизму и радикализации в виртуальном пространстве интернета будет иметь действенный эффект. В данной системе должны присутствовать и своевременное реагирование, и блокировка противоправного контента, и полноценное сотрудничество всех заинтересованных сторон в формировании и распространении позитивного контента, и формирование того самого критического мышления среди пользователей интернета.

Ключевые слова: новые медиа, экстремизм, критическое мышление, радикализация, сетевые сообщества, конвергентная культура, пузыри фильтров, эхо-камера, коммуникативное пространство, противодействие экстремизму.

Коммуникативное пространство современных новых медиа является оптимальной средой для активного распространения нарративов и идеологем экстремистских течений. Преимущественно горизонтальная система социальных взаимодействий в цифровом пространстве позволяет экстремистским течениям и сообществам находить единомышленников и позволять им участвовать в процессах воспроизводства и распространения радикальных и деструктивных идей. Поэтому именно критическое мышление и его развитие в сознании активных пользователей новых медиа является эффективным инструментом по противодействию данным угрозам. Для понимания комплексности ситуации следует первоначально разобраться с понятиями «экстремизм», «новые медиа» и «критическое мышление».

Термин «экстремизм» является базисным для данной работы как ключевая угроза и проблема исследования. Комплексность проблемы и причинно-следственных связей в развитии экстремизма порождает массу дискуссий среди научного сообщества о едином и в то же время наиболее широком определении. Определенная часть научного сообщества, речь идет о представителях правоведения, склонна ориентироваться исключительно на юридическую трактовку экстремизма, которая предполагает перечень деяний противоправного характера, трактуемых как экстремистские. Юридическими

инструментами здесь выступают Федеральный закон № 114-ФЗ «О противодействии экстремистской деятельности», Стратегия противодействия экстремизму в РФ до 2025 года, а также статьи УК РФ и КоАП РФ.

Другая часть научного сообщества выходит за рамки юридической трактовки и отмечает, что экстремизм выступает в качестве идеологической системы, мобилизационной технологии и совокупности насильственных действий. Течения и сообщества экстремистской направленности представляют собой особые социальные миры, фундаментальным способом включения членов социума в которые является специфическая предметная деятельность по насильственной деконструкции социального порядка.

Для экстремизма характерны крайняя степень нетерпимости к оппоненту и стремление к его ликвидации; категорическое неприятие действующих правовых и социальных норм как регуляторов ненавистного социально-политического порядка; излишняя склонность к противоправным действиям насильственного характера, которые экстремистами воспринимаются как единственно верный способ для победы над собственным противником; неприятие гражданских прав и свобод как таковых. Идеальная картина мира экстремиста — общество без физического присутствия ненавистных ему социальных групп; общество, реконструированное согласно его мировоззренческой системе.

Экстремизм — сложное явление, включающая в себя и мировоззрение, и идеологическую систему, и совокупность практических действий по внедрению этой ценностной системы в жизнь. Экстремизм как идеология в любой своей форме имеет примерно идентичную базу когнитивных концептов, например, идеи о неполноценности иных групп, идеи о необходимости спасения и очищения общества от иных групп и так далее. Однако любая форма экстремизма в то же время уникальна и требует при изучении персонального подхода в силу разного комплекса причинно-следственных связей и набора акторов.

Следующий концепт, требующий определения — «новые медиа». Это абсолютно новая форма существования масс-медиа, предполагающее постоянную доступность на цифровых устройствах пользователей и активное участие самих пользователей в создании, трансформации и распространении контента. Новые медиа обладают следующими специфическими чертами:

- отсутствие ограничения интернет-средой и переход онлайн-коммуникации в режим оффлайн;
- интерактивность между пользователями и производимым контентом. В новых медиа под интерактивностью понимается способность цифровой системы незамедлительно реагировать на пользовательские действия, результатом чего становится изменение контента: его содержимого и самой формы контента;
- мультимедийность формата, позволяющая существовать контенту одновременно в разных формах: текст, видеофайл, подкаст и т. д.

Новые медиа обладают с двойственным характером: с одной стороны, они представляют собой следствие технологических экспериментов и стремительного изменения информационных форматов. С другой стороны, новые медиа является некой

синтетической формой или сложной системой взаимодействия традиционных форм медиа и новаторских технологических механизмов [1].

Наличие данных черт есть следствие эволюции новых медиа сквозь призму конвергенции как усиления взаимосвязанности культурных полей и технологий масс-медиа по производству и распространению контента. Благодаря конвергенции новые медиа детерминируются посредством наличия коллективного интеллекта, совершенствования технологий обратной связи и доминирования патриципаторной культуры. Конвергенция происходит на нескольких уровнях сразу: на уровне технических устройств; на уровне компонентов масс-медиа. По своей сути конвергенция является закономерным результатом следующих уровней интеграции [4]:

- интеграция ролей авторов и читателей;
- интеграция ролей авторов и читателей в функционале пользователей;
- интеграция ролей производителей и пользователей в партнерских проектах;
- интеграция ролей производителя и пользователя в функционале пользователя;
- интеграция возможностей создания и восприятия контента в едином инструменте;
- интеграция возможностей работы с контентом и возможностей трансформировать сам инструмент работы.

Закономерным результатом процессов конвергенции в виртуальном пространстве новых медиа становится радикальное изменение места и функционала самого потребителя информационных ресурсов. Теперь потребитель одновременно и распространитель, и создатель, и трансформатор контента. Поэтому колоссально значение приобретает развитие критического мышления в силу того, что неподготовленный пользователь без критического осмысления информации способен продуцировать новые информационные потоки, усиливающие экстремистские течения и радикальные деструктивные нарративы.

Понятие «критическое мышление», подобно другим концептам социогуманитарных наук, не имеет единого определения в силу многостороннего изучения в рамках различных научных направлений. В узком смысле под критическим мышлением понимается корректная оценка поступающих утверждений. Расширенное определение предполагает указание системности процесса анализа, синтеза, оценки и применения полученной извне информации посредством коммуницирования или самостоятельных размышлений. Три основных подхода к изучению критического мышления сложились в западных странах: философский, когнитивный и прикладной; однако такое разделение несколько условно в силу тесной взаимосвязи и взаимозависимости.

Структура критического мышления состоит из двух главных компонентов:

- диспозиция (поиск фундаментов для мировоззрения, проявление открытости и любознательности, демонстрация интеллектуальной независимости и постоянная готовность к вступлению в дискуссии и конструктивные споры);
- умения и навыки по идентификации проблем и путей их решения; оценке аргументов оппонентов; сбору, анализу и верификации информации; выстраиванию причинно-следственных связей; детекции когнитивных искажений и минимизации их влияния на мышление.

Критическое мышление является механизмом, представляющим собой определенный процесс рассуждения. В рамках данного процесса пользователь новых медиа использует целеполагание, выявляет и определяет ключевые проблемы, выдвигает возможные гипотезы, собирает доказательную базу, приводит аргументы *pro et contra*, строит выводы, прогнозирует развитие событий [2].

Критическое мышление как система навыков включает в себя: умение идентифицировать проблему, а также пути для ее решения; умение собирать и систематизировать информацию, оценивать ее с точки зрения достоверности; умение интерпретировать факты и новости; умение адекватно воспринимать используемые языковые средства; умение корректно устанавливать причинно-следственные связи и делать правильные суждения. Использование инструментов критического мышления предполагает следующие этапы при работе с информацией:

- внимательное изучение источника информации с целью установления достоверности или недостоверности. Однако всегда следует помнить, что авторитетность источника информации не является абсолютной гарантией достоверности сведений;
- поиск первоисточника информации, а также идентичной информации из альтернативных источников для последующего сопоставления;
- анализ эмоционального фона информации.

Почему так важно использовать критическое мышление в сфере противодействия влиянию деструктивных идеологий в сетевом пространстве новых медиа? Отсутствие элементарных навыков критического мышления рискует усилить в сознании пользователя когнитивные искажения. Когнитивные искажения представляют собой совокупность систематических ошибок в процессе суждения и мышления в целом, которые возникают на основе неправильных и искаженных убеждений, которые внедрены в когнитивные схемы и оказывают влияние на восприятие человека в определенной ситуации. Мышление человека или пользователя, которое подвергается постоянному влиянию экстремистских идеологов, рискует трансформироваться в мышление по заданным (но, при этом, ошибочным) шаблонным моделям, которые в условиях широкого распространения в социальных медиа эхо-камер и пузырей фильтров будут постоянно укореняться.

Существуют риски стать жертвой воздействия двух коммуникативных практик при взаимодействии с экстремистским контентом: «пузырь фильтров» и «эхо-камера». Пузырь фильтров — это негативный аспект персонализированного поиска, когда интернет-ресурсы выдаются в поисковых результатах на основании ранее изучаемой пользователем информации. А эхо-камера — это ситуация, в которой определенные идеи и концепты усиливаются и закрепляются в сознании пользователя путем повторения и передачи информации. Внутри экстремистских и радикальных сообществ в социальных сетях это очень мощные инструменты, радикализирующие сознание пользователя [3].

Таким образом, результативное противодействие экстремистским проявлениям в пространстве новых медиа обеспечивается за счет целого комплекса мер: своевременное реагирование органов государственной власти с целью пресечения распространения противоправного контента и деятельности деструктивных сообществ; создание и распространение позитивного контента; формирование критического мышления

пользователей новых медиа для пресечения возможной радикализации на начальном этапе. Однако последняя указанная мера достигает эффективности только благодаря регулярному использованию самими пользователями необходимых инструментов анализа информации: критическое отношение к информации; умение отличать достоверные сведения от недостоверных; игнорирование деструктивной информации; своевременная детекция манипуляции; минимизация взаимодействия с нежелательными персонами; использование технического инструментария социальных сетей и интернет-платформ для обеспечения безопасности.

Библиографический список:

1. Евдокимов В.А. Новые медиа как система [Электронный ресурс] // Наука о человеке: гуманитарные исследования. — 2019 г. — URL: <https://cyberleninka.ru/article/n/novye-media-kak-sistema> (дата обращения: 07.12.2020)
2. Коньков С.В. Взаимосвязь критического мышления и медиакомпетентности [Электронный ресурс] // Экономика и бизнес: теория и практика. — 2019 г. — URL: <https://cyberleninka.ru/article/n/vzaimosvyaz-kriticheskogo-myshleniya-i-mediakompetentnosti> (дата обращения: 07.12.2020)
3. Поделуев С.П., Подшибякина Т.А. О факторах политической радикализации в сетевой коммуникации посредством «эхокамер» [Электронный ресурс] // Научная мысль Кавказа. — 2018 г. — URL: <https://cyberleninka.ru/article/n/o-faktorah-politicheskoy-radikalizatsii-v-setevoy-kommunikatsii-posredstvom-ehokamer> (дата обращения: 15.12.2020)
4. Якубенко Е.Н. Конвергенция как фактор формирования современного медиарынка [Электронный ресурс] // Вестник Брянского государственного университета. — 2015 г. — URL: <https://cyberleninka.ru/article/n/konvergentsiya-kak-faktor-formirovaniya-sovremennogo-media-rynka> (дата обращения: 07.12.2020)

References:

1. Evdokimov V.A. New media as a system [Electronic resource] // Science about man: humanitarian studies. - 2019 - URL: <https://cyberleninka.ru/article/n/novye-media-kak-sistema> (accessed: 07.12.2020) (In Russ.)
2. Konkov S.V. The relationship of critical thinking and media competence [Electronic resource] // Economics and Business: Theory and Practice. - 2019 - URL: <https://cyberleninka.ru/article/n/vzaimosvyaz-kriticheskogo-myshleniya-i-mediakompetentnosti> (accessed: 07.12.2020)
3. Kissleyev S. P., Podshibyakina T. A. On the factors of political radicalization in network communication through "echo chambers" [Electronic resource] // Scientific Thought of the Caucasus. - 2018 - URL: <https://cyberleninka.ru/article/n/o-faktorah-politicheskoy-radikalizatsii-v-setevoy-kommunikatsii-posredstvom-ehokamer> (accessed: 15.12.2020)
4. Yakubenko E.N. Convergence as a factor in the formation of the modern media market [Electronic resource] // Bulletin of the Bryansk State University. - 2015 - URL: <https://cyberleninka.ru/article/n/konvergentsiya-kak-faktor-formirovaniya-sovremennogo-media-rynka>

Sergey V. Ventsel

**CRITICAL THINKING FORMATION AS A TOOL TO COUNTERING EXTREMISM
IN THE AGE OF NEW MEDIA**

This article actualizes the problem of critical thinking formation as an effective tool to countering processes of radicalization in the Age of the New Media is actualized by the author. The author sets out the need to understand the structure of critical thinking mechanisms to emphasize the practical benefits in the specific communicative space of New Media. The author emphasizes the key features of New Media as a space of unlimited creativity for all users. At the same time the author notes several actual theoretical and methodological difficulties in resolving the problem, namely the lack of a unified approach to understanding the essence of extremism and ongoing scientific discussions about the essence of new media. The author concludes that only a comprehensive system of countering extremism and radicalization in the virtual space of the Internet will have an effect. This system should include timely response and blocking of illegal content, full cooperation of all stakeholders in the formation and dissemination of positive content, the formation of that very critical thinking among Internet users.

Keywords: new media, extremism, critical thinking, radicalization, online communities, convergent culture, bubble filters, echo-chambers, communicative space, countering violent extremism.

Сведения об авторе:

Венцель Сергей Владимирович, Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет, аналитик.

Адрес электронной почты: ventsel@ncpti.ru

About the author:

Sergey V. Ventsel, the National center of informational countering terrorism and extremism in educational environment and Internet, analyst.

Email: ventsel@ncpti.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ В ОБЛАСТИ КОМПЬЮТЕРНОЙ ТЕХНИКИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ВРЕДНОСНЫХ ПРОГРАММ

ГОРБУНОВА Е.Ю., ХОМИН Д.М.

В последние годы все чаще совершаются посягательства на денежные средства граждан, юридических лиц с использованием вредоносных программ («троянов»). В статье рассмотрен механизм совершения мошеннических действий с использованием «троянов», требующих от потерпевшего перечисление денежных средств на номер мобильного телефона, на электронный кошелек и др. Раскрывать эти преступления удается крайне редко. В связи с этим имеется необходимость в исследовании комплекса мер, направленных на выявление основных признаков преступлений рассматриваемой категории, а также на сбор необходимых доказательств, в том числе в цифровом виде.

Отмечается необходимость привлечения лиц, обладающих специальными знаниями с целью получения криминалистически значимой информации, связанной с применением СВТ, программного обеспечения и информационных технологий.

В тексте данной статьи в виде практических рекомендаций, для сотрудников правоохранительных органов, приводится примерный перечень вопросов, выносимых на разрешение СКТЭ, а также предложен подробный алгоритм экспертного исследования, основанный на общих принципах типовой методики СКТЭ.

По результатам проведенного исследования также сделан вывод, что исследование вредоносных программ объективно трудоемко, вследствие чего проводится не во всех экспертных учреждениях, приводятся основные причины.

Основные положения и выводы статьи могут быть использованы в научной, практической деятельности при рассмотрении вопросов раскрытия, расследования преступлений, совершаемых с использованием вредоносных программ.

Ключевые слова: вредоносная программа, мошенничество, специальные знания, цифровые следы преступления, судебная компьютерно-техническая экспертиза, эксперт.

Цифровые технологии, прогресс – неотъемлемая составляющая жизнедеятельности современного человека, развития современного общества. Вместе с этим, ежегодно киберпреступность наносит огромный вред как частным лицам, организациям, так и государствам.

Современных преступников привлекает доступность разнообразного специализированного программного обеспечения, скорость, удобство, анонимность и отсутствие границ в сети Интернет.

Лицам, которые обладают высоким образовательным уровнем, цифровыми компетенциями в целом, знаниями и навыками в области программирования, в частности,

открываются очень большие возможности их использования, в том числе в корыстных целях. Возможность преступника совершать преступное деяние без непосредственного контакта с жертвой, безусловно, затрудняет выявление таких фактов.

Так, в 2019 году мошенники совершили более полумиллиона незаконных операций (576 566) с использованием электронных средств платежа и украли 6,4265 миллиарда рублей – об этом говорится в отчете Банка России¹. Вместе с этим 69 % всех операций без согласия клиентов было совершено в результате проведения операций клиентом банка путем обмана, с использованием методов социальной инженерии, все остальные – иными способами.

Общее количество зарегистрированных преступлений, совершенных с использованием средств вычислительной техники (далее – СВТ), с каждым годом возрастает, их способы становятся все более изощренными. На деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходилось одно из четырех регистрируемых в 2020 году преступлений².

Опубликованная криминальная статистика, к сожалению, не содержит полной информации для оценки реального масштаба преступлений, которые совершаются с использованием СВТ, поскольку многие пострадавшие не обращаются в правоохранительные органы. Тем самым обеспечивается высокий уровень латентности данных преступлений, остается на низком уровне эффективность расследования преступлений в сфере компьютерной информации.

В сложившейся ситуации особое внимание правоохранительных органов необходимо сосредоточить на повышении эффективности расследования.

Сегодня существует множество способов совершения преступных деяний в сфере экономической деятельности, совершаемых с использованием информационных технологий и СВТ, приведем некоторые распространенные:

1. Удаление, модификация, шифрование данных, а также блокирование доступа с требованием перечисления денежных средств.

2. Удаленное управление операционной системой или корпоративной сетью, перехват информации с требованием перечисления денежных средств.

3. Удаленное управление программным обеспечением для дистанционного банковского обслуживания (ДБО) с целью хищения денежных средств с банковских счетов клиентов.

Ухудшение экономической ситуации, уровня жизни населения, вызванные последствиями всемирной пандемии COVID-19, способствовали совершению преступлений указанными способами. Мишенью стали сотрудники и их компьютерная техника, с которой

¹ Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год // Центральный банк Российской Федерации [сайт]. URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения: 30.12.2020).

² Портал правовой статистики Генеральной прокуратуры РФ // [сайт]. URL: http://crimestat.ru/offenses_chart (дата обращения: 30.12.2020).

они были вынуждены работать дистанционно, из дома, фактически не успев подготовить свои СВТ для безопасной работы.

В данной статье мы рассмотрим и проанализируем механизм совершения мошеннических действий с использованием небольшой группы вредоносного программного обеспечения («троянов»), требующего перечисления денежных средств на номер мобильного телефона, на электронный кошелек и др. Данные преступления совершаются в специфической среде – цифровой, предметом указанных преступных посягательств являются денежные средства.

В уголовно-правовой науке существует термин «вредоносная программа» (ст.273 УК РФ), в отношении которого к настоящему моменту не сложилось единообразия в понимании. Можно сказать, что вредоносное программное обеспечение (далее – ПО) – собирательный термин, который обозначает компьютерную программу, способную причинить вред компьютерной системе, путем осуществления вредоносных функций.

Вредоносные программы создаются с умыслом, в том числе и с целью проникнуть в компьютерную систему, нанести вред, а в большинстве случаев – получить денежные средства.

Следует упомянуть, что в уголовном праве принято считать, что вредоносность программного обеспечения – категория юридическая.

При использовании вредоносных программ, проникновение их на персональный компьютер (далее – ПК) может осуществляться следующими способами: через Интернет, через съемный носитель (SD-карта, внешний НЖМД, usb-флеш накопитель и др.), локальную сеть, используя самые разные методы атаки.

Заражение через Интернет, пожалуй, самый распространённый путь распространения вредоносных программ. Вредоносные программы могут проникать на компьютер, когда просматриваются веб-сайты, загружаются программы из непроверенных источников, открываются вложения сообщений электронной почты и др. Это может произойти в различной ситуации на устройстве, в том числе и при наличии современного антивирусного программного обеспечения с актуальными базами, но шансов проникновения в таком случае гораздо меньше. Вместе с тем планы разработчиков вредоносных программ не были бы успешными, если бы не пользователь, который сам открывает сообщения электронной почты и при просмотре вложений запускает на исполнение вредоносный объект.

Приведем примеры. Первый: «XX.XX.XX года главный бухгалтер ООО «XXXXX» XXXXX, обнаружила, что вследствие вирусной атаки, файлы на компьютере ООО «XXXXX» оказались зашифрованы. Заражение произошло через электронное письмо с вложением. Кто его отправитель, откуда и когда оно было направлено, достоверно не известно. Со слов XXXXX, письмо пришло с Банка XXXXX с вложением, она его открыла, открытие не удалось, на следующий день она обнаружила, что программы не запускаются. Зашифрованными оказались большая часть файлов пользователя на диск «Е»».

Второй: «Не позднее 12 часов 52 минут XX.XX.XX года на адрес электронной почты «xxxxxx@mail.ru» персонального компьютера SPARK установленного в ГОБУЗ «XXXXX» поступило электронное письмо от адресата «XXXXX» (электронная почта «alekshops@xxx.ru»), после прочтения которого произошла блокировка системы с предложением перейти на сайт «Shenge.org» и для разблокировки системы произвести оплату в размере 20000 рублей».

При обращении в техподдержку, например, «Лаборатория Касперского» потерпевшие не получают необходимой помощи, получая электронное письмо с текстом: «мы работаем над этим вопросом, о результатах уведомим по почте».

В приведенных нами примерах пришло письмо на электронную почту вероятно от известного контрагента (либо со схожим наименованием) с просьбой, например, подтвердить оплату по счету, произвести бухгалтерскую сверку, оплатить штрафы или др. Информация всегда такова, что непременно заинтересует получателя письма и он откроет вложение. Далее, механизм проникновения вредоносной программы в операционную систему ПК может выглядеть следующим образом. После того, как пользователь открыл вложение с файлом «schet.zip», содержащим файл с расширением «js» (является Javascript (мультипарадигменный язык программирования)), скрипт загружает с сайта вредоносную программу, далее она исполняет заложенную задачу–алгоритм, реализующий исполнение следующих функций: уничтожение, шифрование файлов, блокирование доступа к ним и др.

Главное отличие вредоносных программ от каких-либо других программ в том, что все действия после их запуска происходят скрытно, без уведомления пользователя.

Вредоносные программы распространяются людьми и обнаруживаются в момент, когда явно проявляются последствия их применения, либо путем сканирования антивирусным программным обеспечением¹ как непосредственно компьютерной системы, так и носителей информации.

Следует отметить и сложность квалификации преступлений, совершаемых с использованием вредоносного программного обеспечения («тroyанов»). Связано это прежде всего со способом совершения преступления, который состоит из нескольких этапов:

- создание вредоносного программного обеспечения, образует состав преступления, предусмотренного ст.273 УК РФ;

Рассматриваемое вредоносное программное обеспечение по своему функционалу имеет цель–лишить пользователя возможности доступа к файлам, шифруя их, не позволяя получить доступ к компьютерной информации, которая в них находится.

- отправка вредоносной программы конкретному получателю, с явным умыслом (распространение происходит различными способами);

- неправомерный доступ к компьютерной информации: проникновение в компьютерную систему и воздействие на ее объекты (уничтожение, блокирование, модификация).

¹ Антивирусное программное обеспечение–антивирусные пакеты от компаний: «Лаборатория Касперского», «Доктор Веб», «ESET» и др. с базами актуальными на момент исследования.

В связи с данным обстоятельством, для потерпевшего может наступить нарушение деятельности, причинение материального ущерба и др.

– после незаконного воздействия вредоносной программы на файлы (наступление последствий), требование уплаты денежных средств в указанный период времени путем перевода в соответствии с предложенной инструкцией. Одновременно нередко присутствует угроза о том, что если денежные средства не будут перечислены, зашифрованные файлы могут быть уничтожены;

Поскольку рассматриваемое вредоносное программное обеспечение требует уплаты денежных средств, то действия разработчиков программ ввиду материальной, корыстной заинтересованности, могут быть квалифицированы в соответствии с ч.2 ст. 273 УК РФ.

Наличие угрозы в виде утраты информации и ограничения времени для перечисления денежных средств можно квалифицировать и как мошенничество, и как вымогательство.

Потерпевшие могут перечислять денежные средства не из-за угрозы, а фактически из-за обмана, в соответствии с предложенной инструкцией, поскольку не владеют необходимыми и достаточными знаниями, чтобы оценить обстановку, полагая, что после уплаты требуемой суммы, им пришлют код для расшифровки, восстановления файлов. Личный контакт между преступником и потерпевшими отсутствует, но потерпевший не лишен права выбора: платить или не платить. Поэтому, действия преступников, основывающиеся на обмане, могут быть квалифицированы в соответствии с ч. 1 ст. 159.6 УК РФ.

Поскольку указанные преступления совершаются в цифровой среде, имеющей специфический механизм и особое слеодообразование, правоприменитель обращается за помощью к лицам, обладающим специальными знаниями с целью получения криминалистически значимой информации, связанной с применением СВТ, программного обеспечения и информационных технологий,

Важной и основной процессуальной формой использования специальных знаний в расследовании преступлений, совершаемых с использованием вредоносных программ является судебная компьютерно-техническая экспертиза (СКТЭ), более точно – программно-компьютерная экспертиза (вид СКТЭ), которая может назначаться в экспертные подразделения МВД России.

Целью программно-компьютерной экспертизы является установление причастности исследуемого программного обеспечения к расследуемому преступному деянию, обнаружение цифровых следов его использования на носителях компьютерной информации, где непосредственно наступил результат неправомерного доступа, вредоносного воздействия.

На исследование поступают как персональные компьютеры, так и различные устройства, содержащие информацию в цифровом виде, эксперту могут быть поставлены следующие вопросы (приведены примеры вопросов из постановлений о назначении экспертизы):

1. Имеются ли на представленном на исследование накопителе на жестком магнитном диске (НЖМД) системном блоке персонального компьютера (СБ ПК) какие-либо программы, являющиеся вредоносными (заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети), если да то какие и когда они были установлены?

2. Имеется ли на НЖМД СБ ПК программное обеспечение, предназначенное для несанкционированного шифрования данных? Если да, то, когда оно установлено (размещено) и имеются ли сведения о его использовании (протоколы работы)?

3. Какие данные (файлы) были стерты (уничтожены, скопированы, изменены (модифицированы)? Как изменялось их содержание, дата создания (уничтожения изменения)?»

4. Из какого источника на носитель было занесено данное программное обеспечение?

Стоит отметить, что не все из указанных вопросов могут быть разрешены в ходе производства СКТЭ. Недостаточный уровень общих и узкоспециальных знаний в области компьютерной техники и информации у правоприменителей приводит к постановке некорректных с правовой и технических точек зрения вопросов эксперту, в т.ч. выходящих за пределы его специальных знаний. Вследствие чего исследование проводится длительно, а ответы эксперта по таким вопросам не вносят ясность в расследовании. Вместе с тем, от правильной постановки вопросов и ответов на них зависит последующая квалификация преступного деяния, планирование дальнейших действий следователя.

Существующие сегодня рекомендации по обнаружению, фиксации, изъятию и исследованию цифровых следов носят фрагментарный характер, а методики производства судебных экспертиз нуждаются в актуализации [1; 2], поэтому эксперт разрабатывает частную методику исследования, основываясь при этом на общих принципах типовой методики СКТЭ.

В ходе исследования вредоносных программ применяются следующие основные экспертные методы, соответствующие поставленным задачам:

- исследование программных алгоритмов;
- исследование дизассемблированного кода;
- мониторинг действий и поведения в операционной системе, анализ взаимодействия с локальными файлами, сетевое взаимодействие.

Приведем общий алгоритм исследования, основанный на указанных методах, который можно использовать в СКТЭ как основу для ответа на поставленные вопросы:

1. НЖМД извлекается, подключается к аппаратно-программному комплексу эксперта с блокировкой записи (аппаратной либо программной).

2. Информация с исследуемого НЖМД с помощью специализированного программного обеспечения (например, «AccessData FTK Imager») копируется на НЖМД эксперта в файл-образ. Дальнейшее исследование проводится с использованием копии НЖМД, представленного на исследование.

3. В зависимости от обстоятельств проводится восстановление удаленных файлов.

4. Осмотр и анализ объектов файловой системы с целью обнаружения измененных (зашифрованных) файлов. На данном этапе устанавливаются факты модификации файлов, которые подверглись воздействию вредоносной программы. В каждом конкретном случае, на исследуемых носителях информации может быть обнаружено разное количество зашифрованных (модифицированных) файлов.

Например, вирус-шифровальщик «Vault» шифрует пользовательские данные, заменяя популярным типам файлам с стандартное расширение с: «doc», «docx», «xls», «xlsx», «jpeg», «pdf» и др. на «*.vault». Эта вредоносная программа использует режим шифрования, практически исключающий возможность подбора ключа для самостоятельной расшифровки файлов. Простое переименование файла не помогает.

5. Сканирование объектов файловой системы, имеющихся на исследуемом носителе информации с использованием антивирусного программного обеспечения, находящегося в распоряжении эксперта.

Для сканирования рекомендуется использовать несколько антивирусных программных продуктов. Это могут быть, например, антивирусные программы от компаний: «Лаборатория Касперского», «Доктор Веб», «ESET» и др. с базами актуальными на момент исследования.

В результате проделанных действий могут быть обнаружены файлы, детектируемые специализированным программным обеспечением (рис.№1), сведения о которых сводятся в таблицу (табл.№1). В заключении приводятся все сведения об обнаруженных угрозах и предупреждениях.

Особенностью такого способа обнаружения вредоносного программного обеспечения является то, что антивирусные программы работают с исходным кодом, не затрагивая его поведение.

Защищено: Trojan-Ransom.Win32.Crusis.to	L:\Documents and Settings\user\Local\Programs\Internet Explorer\..._back\..._...	
Обнаружено: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\Videos\A1283Hlo.exe	
Создана резервная копия: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\A1283Hlo.exe	
Создана резервная копия: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\AppData\Roaming\A1283Hlo.exe	
Создана резервная копия: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\Videos\A1283Hlo.exe	
Невозможно удалить: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\A1283Hlo.exe	Не п
Невозможно удалить: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\Videos\A1283Hlo.exe	Не п
Невозможно удалить: Trojan-Ransom.Win32.Crusis.to	L:\Users\test\AppData\Roaming\A1283Hlo.exe	Не п
Не обработано	L:\Users\usr\AppData\Local\History	Дос
Не обработано	L:\Users\usr\AppData\Local\Temporary Internet Files	Дос
Не обработано	L:\Users\usr\AppData\Roaming\Microsoft\Windows\Start Menu\Программы	Дос

Рисунок №1. Информация об обнаруженных файлах в результате работы программного продукта от «Лаборатория Касперского»

Название и путь к файлу	Размер (дата создания)	Наименование программы согласно классификации «Лаборатория Касперского»	Наименование программы согласно классификации «ESET»	Наименование программы согласно классификации «Доктор Веб»
<НЖМД_Раздел2>:\Users\test\AppData\Roaming\A1283Hlo.exe	4 540 байт 06.06.2020 г., 9:58:43	Trojan-Ransom.HTML.Agent.b	Win32/Filecoder.FH	не определен

Таблица 1 Информация о файлах, детектируемых программами-антивирусами

Основу рассматриваемой нами группы вредоносных программ составляют различные вариации вирусов типа «Trojan»¹. В настоящее время антивирусные программы (с актуальными базами) в большинстве случаев распознают и блокируют вирусы данного типа, но если на ПК отсутствует антивирусное программное обеспечение, то происходит заражение.

6. Далее эксперт изучает, анализирует информацию о файлах, обнаруженных на предшествующем этапе.

Рассмотрим для приведенного нами примера №1.

В результате поиска антивирусной программой, на НЖМД СБ ПК было обнаружено 4 файла: «rad4D3B1.tmp», «rad39CA1.tmp», «radD17BE.tmp» (раздел №1:\Documents and Settings\Admin\Local Settings\Temp), определяемые как «Trojan.Win32.Inject.adwaz» и файл «schet_xls.js» (раздел №1:\Downloads\Архивы\schet.zip/), определяемый как «HEUR:Trojan.Script.Agent.gen», информация о которых приведена в таблице №2.

N №	Имя файла	Атрибуты		Логический размер (байт)	Значение хэш-функции SHA-1 ²
		Дата и время создания	Дата и время изменения		
11.	schet_xls.js	-	06.03.2020 12:27	19 029	9a7bad4f1a0e4bf57950edd42c28c24cfaa37373
22.	rad4D3B1.tmp	06.03.2020 15:51	06.03.2020 15:51	941 549	954bab6058af63b88ca358c9d12664a6d9d55573
33.	rad39CA1.tmp	06.03.2020 15:51	06.03.2020 15:51	941 549	954bab6058af63b88ca358c9d12664a6d9d55573
44.	radD17BE.tmp	06.03.2020 15:51	06.03.2020 15:51	941 549	954bab6058af63b88ca358c9d12664a6d9d55573

Таблица 2 Информация о файлах, отобранных для дальнейшего анализа и исследования

Для характеристики объектов файловой системы (каталоги и файлы), связанных со временем (дата создания, дата модификации), а также времени совершения преступления, используются значения системного времени на момент выполнения с объектами файловой системы каких-либо операций.

Учитывая, что значение контрольных сумм, рассчитанных по алгоритму «SHA-1», а также даты создания для трех исследуемых файлов (№№2-4) в таблице №2 совпадают, можно сделать вывод, что они идентичны по содержанию, дальнейшему анализу и исследованию может быть подвергнут один из этих файлов.

Фактически, на данном этапе происходит обнаружение и отбор объектов (файлов) для дальнейшего анализа. Обнаруженные на данном этапе файлы записываются на оптический диск однократной записи и являются приложением к заключению эксперта.

¹ Trojan– троянская вирусная программа, разновидность вредоносной программы, маскируется под легитимное ПО.

² SHA-1 – алгоритм криптографического хеширования.

7. Статический и динамический анализ отобранных файлов.

Анализ вредоносных программ – это процесс (метод) определения происхождения и потенциального воздействия конкретной вредоносной программы. Для этих целей применяются методы и инструменты статического и динамического анализа. Обнаружение, идентификация и анализ имеют решающее значение в исследовании вредоносных программ.

Статический анализ – анализ файла, его структуры, без его запуска на выполнение.

Динамический анализ включает в себя запуск вредоносной программы, ее идентификацию, наблюдение за ее действиями и поведением в операционной системе, анализ взаимодействия с локальными файлами, сетевое взаимодействие.

Динамический анализ проводится с использованием изолированной виртуальной среды, которая эмулирует оборудование, доступ к сети Интернет, команды чтения/записи в файлы и др., но в то же время не позволяет вредоносной программе вносить изменения в работающую операционную систему ПК эксперта. Для этих целей может использоваться, например, комплекс следующего программного обеспечения: «Sandboxie» «Buster Sandbox Analyzer», «VMware Workstation «Microsoft Windows 7», «Wishark», «Microsoft Network Monitor» и др.

Для дизассемблирования¹ исполняемых файлов, отладки исполняемых файлов и порождаемых ими процессов, мониторинга изменений файловой системы, реестра операционной системы, может использоваться следующее программное обеспечение: отладчик «ollydbg», утилиты «sysinternals suite» и др.

В нашем примере, в ходе исследования файла «schet_xls.js» было установлено следующее:

- просмотром содержимого файла «schet_xls.js» выявлено, что он содержит код JavaScript, который подвергнут обфускации²;
- во время исполнения кода проверяет наличие двух удаленных адресов: «myo2.net», «asec.netcom-activ.ro». При доступности данных адресов, загружает с этих адресов файл с именем «winconfig.exe» (рис.№2);

```
GET /uploads/contracte/options/x7czd/papkaa17/winconfig.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; .NET4.0C; .NET4.0E)
Host: asec.netcom-activ.ro
Connection: Keep-Alive

GET /eclean/data/file/product/thumbOpen/winconfig.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
```

¹ Дизассемблирование – преобразование файла в текст программы на языке ассемблера.

² Обфускация – запутывание кода, т.е. приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ при декомпиляции.

SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)

Host: **myo2.net**

Connection: Keep-Alive

Рисунок №2. Запросы на загрузку файла «winconfig.exe», отправленные при выполнении скрипта «schet_xls.js».

–после загрузки файла «winconfig.exe» в каталог «\Users\«имя пользователя»\AppData\Local\Temp\», исполняет его с именем «rad*****.tmp», где ***** - 5 случайных символов;

–после выполнения кода, удаляет файл «schet_xls.js».

В ходе исследования файла «rad4D3B1.tmp» было установлено следующее:

–при просмотре сигнатуры¹ и структуры файла «rad4D3B1.tmp» было установлено, что он является исполняемым;

–при запуске файла «rad4D3B1.tmp» (при выполнении скрипта) копирует сам себя в каталог «<НЖМД>:\ProgramData\Windows\», при этом изменяет свое имя на «csrss.exe»;

–для автоматического запуска при каждой последующей загрузке операционной системы записывает свои параметры в реестр операционной системы по адресу «Software\Microsoft\Windows\CurrentVersion\Run» (рис.№3);



Рисунок №3. Фотоизображение ветви реестра операционной системы.

– записывает свои параметры в реестр операционной системы «SOFTWARE\System32\Configuration», в том числе полученные сведения об имени компьютера, собирает сведения о теневых копиях;

– с помощью утилиты «vssadmin.exe», предназначенной для администрирования службы теневого копирования томов (средства «Microsoft Windows 7 Ultimate»), удаляет теневые копии;

– пытается установить соединение по протоколам «http» и «https» со следующими IP-адресами²: «171.25.193.9», «154.35.32.5», «131.188.40.189», «194.109.206.212»;

– изменяет (зашифровывает) файлы со следующими расширениями: cdr, srw, mdf, txt, xml, csv, pdf, xl, xls, xlsx, docx, doc, avi, mkv, mov, mp4, и др.;

– создает файлы с расширением «no_more_ransom», изменяя также имя файла, пример – «CRm8BrKHH0pTOus3NQbUD1zanBq-7NwJfO-N 0+zueVHyBeDMCa7pIxaqiq1Хyb-ObaRZMV7JBLgJ8MdXB1lg==.A3D1A8E615542DE7862D.no_more_ransom»;

– по окончании изменения (шифрования) пользовательских файлов, копирует файл «15BD342B15BD342B.bmp», содержащий графическое изображение, в каталог «<НЖМД>:\Users\«имя пользователя»\AppData\Roaming\».

¹ Сигнатура– список данных, используемых для идентификации или проверки содержимого файла.

² IP-адрес– уникальный сетевой адрес узла в компьютерной сети, построенной на основе протокола IP.

Требование выводится на экран в виде текста, для России – на русском языке (рис.№4).

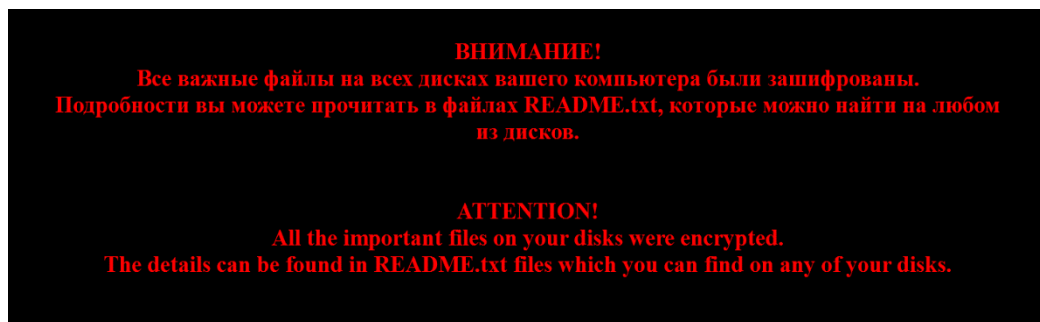


Рисунок №4. Фотоизображение сообщения, которое видит пользователь.

Также создаются текстовые файлы с именем «README*.txt», где «*»– числовое значение. В файле содержатся инструкция для пользователя, приведена на рис.№5.

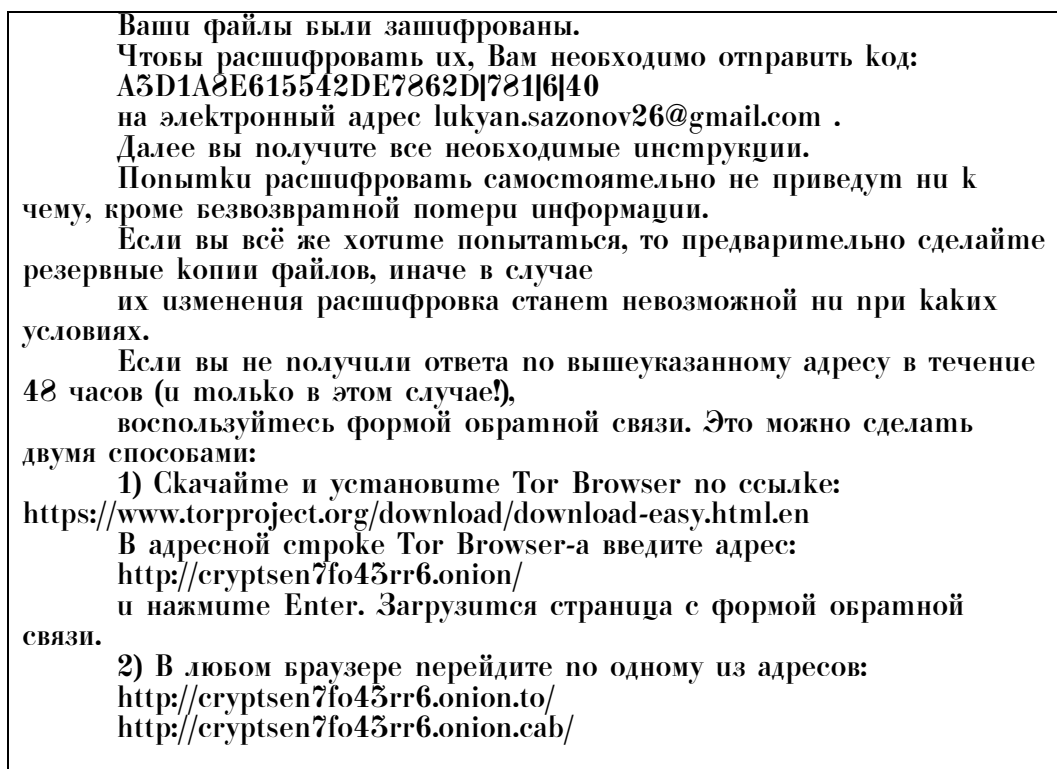


Рисунок №5. Фрагмент содержимого файла «README*.txt».

Основу выдвигаемых требований составляют обман, именно на этом построена схема данного преступления. Объединяет все подобные вредоносные программы требование перевести денежные средства согласно предложенной инструкции в указанный период времени.

8. На следующем этапе исследования осматриваются системные файлы и каталоги, объекты файловой системы с целью:

–исследования истории интернет-браузеров, в том числе среди удаленной информации;

–исследования сохраненных и доступных для извлечения сообщений программ, предназначенных для обмена электронной почтой, в том числе среди удаленной информации;

–изучения механизма, с помощью которого файлы, указанные в таблице №2, попали на НЖМД СБ ПК;

Просмотром содержимого файлов: «<НЖМД_Раздел №1>:\Documents and Settings\Admin\Local Settings\Application Data\Mozilla\Firefox\Profiles\k7wui19f.default\cache2\entries\0470F9E697FF83531BDBB8F9845754D66C21D209», «<НЖМД_Раздел №1>:\Documents and Settings\Admin\Application Data\Download Master\temp\URLComboBox.hnt» и др. установлено, что файл с именем «schet.zip» был загружен с интернет -ресурса «<http://gallery.compot.ru>» не позднее 06.03.2017 12:27 (табл.№2).

Осмотр истории интернет -браузеров может проводиться как ручным способом, с использованием различных утилит, так и с использованием криминалистического программного обеспечения, например, «Belkasoft Evidence Center Ultimate».

В большинстве случаев, обнаруженные экспертом цифровые следы являются единственной возможностью восстановить механизм совершения рассматриваемых преступлений, а также собрать доказательства: список файлов, подвергшихся воздействию (шифрованию); интернет-ресурс, с которого было загружены вредоносные программы; дату загрузки; адрес отправителя электронной почты, с которой было отправлено письмо с вложением; IP-адреса, с которыми происходит взаимодействие; предъявляемые требования, а также электронный адрес, криптокошелек, киви-кошелек, номер телефона, которые могут быть указаны в инструкции; установить функциональное назначение программного обеспечения, механизм распространения в операционной системе и оставляемые артефакты и др.

В каждом конкретном случае количество собранных доказательств разное и зависит прежде всего от:

–от алгоритма, заложенного в программный код вредоносной программы, в ходе исполнения которого могут быть удалены следы воздействия (несанкционированного доступа);

–фиксации информации в СБТ, подвергшегося воздействию вредоносных программ, а также быстроты изъятия СБТ. Нередко пользователи, а также администраторы, специалисты по безопасности вносят безвозвратные изменения в цифровые следы, что приводит к утрате (уничтожению) криминалистически значимой информации;

Таким образом, заключение СКТЭ может сыграть определяющую роль при производстве расследования.

В соответствии с приведенными примерами обстоятельств совершения преступлений, предложенным алгоритмом исследования, на наш взгляд, можно определить примерные вопросы, выносимые на разрешение СКТЭ:

1.Имеются ли на представленном СБ ПК программы, детектируемые антивирусным программным обеспечением?

2. Имеются ли сведения о загрузке на НЖМД СБ ПК файлов, обнаруженных при ответе на вопросе №1?

3. Возможно ли с использованием программного обеспечения, обнаруженного при ответе на вопросе №1 произвести шифрование, модификацию, удаление файлов?

4. Возможно ли восстановить информацию, содержащуюся в файлах, подвергшихся шифрованию, модификации?

Приведенный перечень вопросов не исчерпывающий, безусловно, зависит от конечной цели исследования и обстоятельств расследуемого события.

Приведенный нами алгоритм исследования, статического и динамического анализа, а также практический опыт авторов, позволяют утверждать, что исследование вредоносных программ объективно трудоемко, вследствие чего проводится не во всех экспертных учреждениях.

Обусловлено это рядом причин, приведем основные:

Во-первых, СКТЭ – один из видов инженерно-технических экспертиз, где до настоящего времени окончательно не определено видовое деление. Видовое деление и задачи являются до настоящего времени предметом самых горячих дискуссий в научной среде.

В разных ведомствах нормативно закреплён перечень проводимых экспертиз, так, в экспертно-криминалистических подразделениях органов внутренних дел РФ проводится «Компьютерная экспертиза. Исследование компьютерной информации»¹, а в судебно-экспертных учреждениях Минюста России – «Компьютерно-техническая экспертиза. Исследование информационных компьютерных средств»².

Отсутствие единого видового деления, методического обеспечения и подготовленных сотрудников приводят к тому, что программно-компьютерные экспертизы³ (вид СКТЭ) в органах внутренних дел производятся фактически при производстве «компьютерной экспертизы».

Вместе с тем правильное название экспертных исследований важно, как при назначении экспертизы следователем, так и в процессе проведения судебного

¹ Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: Приказ МВД России от 29.06.2005 г. № 511// Российская газета. 2005. 30 августа. № 191.

² 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: Приказ Минюста России от 27.12.2012 г. № 237// Министерство юстиции Российской Федерации [сайт]. URL: <https://minjust.gov.ru/ru/documents/7910/> (дата обращения: 30.12.2020).

³ Программно-компьютерной экспертизой принято называть экспертное исследование программного обеспечения. В данном случае исследуются закономерности разработки и применения программного обеспечения, с использованием эмуляции, виртуализации, мониторинга системных событий, поиска системных аномалий и др.

разбирательства, поскольку это позволяет однозначно и более точно определить: предмет, объект и задачи экспертных исследований.

Во-вторых, исследование вредоносных программ чрезвычайно сложно, состоит из нескольких этапов, длительно.

В экспертно-криминалистических подразделениях МВД России трудятся чуть более 400 экспертов, имеющих право самостоятельного производства «компьютерных экспертиз». Такого количества экспертов явно недостаточно в эпоху цифровизации, а компетенции многих экспертов не позволяют работать с программным кодом, программным обеспечением для статического и динамического анализа. В силу загруженности эксперты не имеют достаточного времени для анализа вредоносных программ, а взаимодействие экспертов с разработчиками специализированного программного обеспечения: «Лаборатория Касперского», «Доктор Веб», «ESET» в рамках служебной деятельности полностью отсутствует.

В-третьих, от уровня оснащенности аппаратно-программными средствами экспертных учреждений, производящих СКТЭ;

В-четвертых, стремится к нулю практика назначения судебных программно-компьютерных экспертиз в организации, которые имеют для этого технические возможности и кадровый потенциал («GroupIB», «Лаборатория Касперского» и др.) и связано это в большей мере высокой стоимостью исследований.

Несмотря на существующие трудности, судебная компьютерно-техническая экспертиза в уголовном процессе востребована, находится в стадии активного развития, способна решать различные задачи, возникающие в ходе расследования преступлений, в том числе в сфере экономической деятельности. Вместе с этим нуждается в подготовке научных исследований в рассматриваемом направлении, методическом обеспечении, в подготовленных кадрах, обладающих специальными знаниями, высоким уровнем компетенций, как в области информационных технологий, так и программного обеспечения, программирования.

Основные положения, приведенные в статье, могут быть использованы как в образовательном процессе, так и в практической деятельности при рассмотрении вопросов раскрытия, расследования, предупреждения преступлений, связанных с использованием СВТ и вредоносных программ.

Библиографический список:

1. Общие положения по назначению и производству компьютерно-технической экспертизы : методические рекомендации / В. С. Зубаха, А. И. Усов, Г. В. Саенко [и др.]. М., 2000. С. 8-15.
2. Саенко Г. В., Тушканова О. В. Типовые экспертные методики исследования вещественных доказательств. Ч. I: Исследование компьютерной информации / под ред. Ю. М. Дильдина; общ. ред. В. В. Мартынова. М., 2010. С. 189-243.

References:

1. General provisions on the purpose and production of computer-technical expertise: methodological recommendations / V.S. Zubaha, A.I. Usov, G.V. Saenko [et.cet.]. M., 2000. P. 8-15. (In Russ.)

Saenko G. V., Tushkanova O. V. Standard expert methods of investigation of physical evidence. Part I: Research of computer information / by ed. Yu. M. Dil'dina; red. V.V. Martynova. M., 2010. P. 189-243. (In Russ.)

Elena Yu. Gorbunova, Dmitry M. Khomin

**CURRENT PROBLEMS THE USE OF SPECIAL KNOWLEDGE IN THE FIELD OF
COMPUTER TECHNOLOGY AND SOFTWARE IN THE INVESTIGATION OF FRAUD
COMMITTED WITH THE USE OF MALWARE**

In recent years, attacks on the funds of citizens and legal entities with the use of malicious software ("Trojans") have been increasingly committed. The article discusses the mechanism of committing fraudulent actions using "Trojans", requiring the victim to transfer funds to a mobile phone number, an electronic wallet, etc. It is infrequently possible to uncover these crimes. In this regard, there is a need to study a package of measures aimed at identifying the constituent elements of offence of the category under consideration, as well as to collect the necessary evidence, including in digital form. It is noted that it is necessary to involve persons with special knowledge in order to obtain criminally significant information related to the use of SVT, software and information technologies.

In the text of this article, in the form of practical recommendations for law enforcement officers, an approximate list is provided. A detailed algorithm of expert research based on the general principles of the standard SCTE methodology is proposed.

According to the results of the study, it is also concluded that the study of malware is objectively time-consuming, as a result of which it is not carried out in all expert institutions, the main reasons are given.

The main provisions and conclusions of the article can be used in scientific and practical activities when considering the issues of disclosure and investigation of crimes committed with the use of malicious programs.

Keywords: malware, fraud, special knowledge, digital traces of crime, forensic computer-technical expertise, expert.

Сведения об авторах:

Горбунова Елена Юрьевна, ЭКЦ УМВД России по Мурманской области, отдел компьютерных экспертиз, эксперт.

Адрес электронной почты: elena_exp@mail.ru

ГОРБУНОВА Е.Ю., ХОМИН Д.М.

Хомин Дмитрий Михайлович, ЭКЦ УМВД России по Архангельской области, отделение компьютерных экспертиз отдел инженерно-технических экспертиз, главный эксперт.

Адрес электронной почты: kdimmm@rambler.ru

About the authors:

Elena Yu. Gorbunova, Department Forensic Science Center Ministry of internal Affairs of Russia in the Murmansk region, Computer Expertise Department, expert

E-mail: elena_exp@mail.ru.

Dmitry M. Khomin, Department Forensic Science Center Ministry of internal Affairs of Russia in Arkhangelsk region, Department computer forensics division of the engineering and technical expertise of the computer, chief expert.

E-mail: kdimmm@rambler.ru.

ПРОБЛЕМНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ИЗГОТОВЛЕНИЯ И ОБОРОТА МАТЕРИАЛОВ ИЛИ ПРЕДМЕТОВ С ПОРНОГРАФИЧЕСКИМИ ИЗОБРАЖЕНИЯМИ НЕСОВЕРШЕННОЛЕТНИХ

ДОРОФЕЕВ К.И.

В статье рассматриваются проблемные вопросы организации и использования специальных знаний при расследовании изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних. С учетом изученной правоприменительной практики, предлагаются меры организационно-методического, правового и материально-технического характера, реализация которых, по мнению автора, будет способствовать более эффективному использованию возможностей судебных экспертиз при расследовании преступлений анализируемого вида.

Ключевые слова: специальные знания, судебная экспертиза, порнографические материалы и предметы с порнографическими изображениями несовершеннолетних.

В условиях перехода Российской Федерацией на новый промышленный уклад, основой которого должна стать цифровая экономика, одним из ключевых направлений указанной деятельности выступает обеспечение информационной безопасности¹.

В соответствии со ст. 6 Стратегии национальной безопасности Российской Федерации под безопасностью следует понимать состояние защищенности личности, общества и государства от внутренних и внешних угроз, в том числе в информационной сфере². В дополнение к этому согласно абз. 5 ч. 1 ст. 4 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее – ФЗ № 436-2010), основным объектом правовой охраны государства определена защита детей от факторов, негативно влияющих на их физическое, интеллектуальное, психическое, духовное и нравственное развитие³.

В рамках взятых Российской Федерацией обязательств в уголовный закон внесены нормы, предусматривающие уголовную ответственность за изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, а также за действия по вовлечению детей в процесс изготовления таких объектов (ст. 242.1, 242.2 УК РФ). Особенность указанных преступлений связана с тем, что они могут выступать

¹ «О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»: Постановление Правительства Российской Федерации от 2 марта 2019 г. № 234 (ред. от 21 августа 2020 г.) // Справочно-правовая система «КонсультантПлюс».

² «О Стратегии национальной безопасности Российской Федерации»: Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 // Справочно-правовая система «КонсультантПлюс».

³ «О защите детей от информации, причиняющей вред их здоровью и развитию»: Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (ред. от 31 июля 2020 г.) // СЗ РФ. 2011. № 1. Ст. 48.

составной частью различных групп преступлений, систематизируемых по следующим основаниям [1]:

- преступления, связанные с оборотом порнографического контента, совершаемых с помощью информационно-телекоммуникационных сетей (далее – ИТКС) (ч. 3 ст. 242, ст. 242.1, 242.2 УК РФ);

- преступления, связанные с насильственными и ненасильственными действиями сексуального характера, совершаемые в отношении малолетних и несовершеннолетних (ст. 131-135, 240, 241 УК РФ).

Актуальность изучения преступлений анализируемого вида связана и с особенностями учета противоправных деяний, фиксируемых МВД России и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор).

Так, в 2018 году по преступлениям, предусмотренным ст. 242.1 УК РФ, зарегистрировано 563 преступления¹. В то время, как за указанный период времени в Роскомнадзор поступило 42 506 обращений о размещении в сети Интернет материалов с порнографическими изображениями несовершеннолетних, что расходится с официально регистрируемой преступностью в десятки раз и свидетельствует о высокой латентности преступлений анализируемого вида [4].

Приведенные статистические данные свидетельствуют о существовании проблемных аспектов, оказывающих непосредственное влияние на эффективность выявления, документирования и расследования преступлений, предусмотренных ст. 242.1 УК РФ. К одному из таких аспектов относятся вопросы организации и использования специальных знаний при расследовании преступлений анализируемого вида.

Основной формой процессуального использования специальных знаний является судебная экспертиза. В ходе изучения законодательства Российской Федерации, а также материалов архивных уголовных дел, возбужденных по признакам ст. 242.1 УК РФ установлено, что по данной категории преступлений зачастую назначаются следующие виды экспертиз:

- судебная экспертиза по исследованию объектов порнографического характера;
- судебная компьютерная экспертиза по исследованию электронных носителей информации, свидетельствующих о нахождении в распоряжении злоумышленника материалов с порнографическими изображениями несовершеннолетних и его причастности к их обороту;

- судебно-психиатрическая экспертиза по установлению у лица в возрасте старше 18 лет, заподозренного в совершении преступления против половой неприкосновенности несовершеннолетнего, не достигшего возраста 14 лет, наличия или отсутствии у него расстройства сексуального предпочтения (педофилии) (п. 3.1 ст. 196 УПК РФ).

Остальные судебные экспертизы проводятся в случае: установления личности жертвы преступления; в зависимости от позиции, заявленной стороной защиты; при

¹ Единый отчет о состоянии преступности по России / Форма 1 ЕГС. ГИАЦ МВД России за 2018 год.

обнаружении и изъятии иных объектов, свидетельствующих о причастности лица к совершенному преступлению.

Рассмотрим более подробно проблемы, возникающие при организации и проведении указанных судебных экспертиз.

Изучение более 300 архивных уголовных дел, возбужденных в период с 2004 по 2020 годы по ст. 242.1 УК РФ, позволило выделить более 20 вариантов названий судебных экспертиз, проводимых в ходе исследования объектов порнографического характера.

Различия в подходах к проведению рассматриваемых исследований, на наш взгляд, связан с отсутствием до настоящего времени утвержденной методологии исследования объектов порнографического характера, тогда как на постсоветском пространстве такие методики существуют¹.

Указанную деятельность был призван упорядочить ФЗ № 436-2010, которым установлен перечень информации, запрещенной к обороту на территории России, а также определены процедура проведения экспертизы информационной продукции и требования к специалистам, которые будут ее проводить. Однако большинство концептуальных вопросов в этой области так и остался не затронутым.

Концепция информационной безопасности детей (далее – Концепция), которую используют аккредитованные Роскомнадзором эксперты при проведении исследования информационной продукции, носит рекомендательный характер. Более того указанный документ не содержит четких пределов по отграничению одного научного знания от другого, которые различаются в зависимости от предмета конкретной научной или учебной дисциплины. Изложенное может привести к выходу экспертом за пределы его компетенции с последующим исключением заключения эксперта из перечня доказательств [2].

К примеру, эксперты, необходимые для исследования порнографических объектов (специалисты в области медицины, педиатрии, сексологии, культуры и искусства), отсутствуют в экспертных учреждениях системы МВД России, Следственного Комитета Российской Федерации, Министерства Юстиции Российской Федерации, что следует из анализа их подзаконных нормативных правовых актов².

¹ Государственный реестр методик судебно-экспертных исследований Республики Казахстан / Сайт информационной системы Параграф «Юрист» [Электронный ресурс] URL: <https://goo-gl.ru/k1Ju5>. Дата обращения: 01.12.2020.

² «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»: приказ МВД России от 29 июня 2005 г. № 511 // Справочно-правовая система «КонсультантПлюс»; «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»: приказ Министерства юстиции Российской Федерации от 27 декабря 2012 г. № 237 (ред. от 13 сентября 2018 г.) // Справочно-правовая система «КонсультантПлюс»; «Об утверждении Порядка определения, пересмотра уровня квалификации и аттестации экспертов федерального государственного казенного учреждения «Судебно-экспертный центр Следственного комитета Российской Федерации» на право самостоятельного производства судебных экспертиз»: приказ Следственного Комитета Российской Федерации от 24 июля 2020 г. № 77 // Справочно-правовая система «КонсультантПлюс».

Следовательно, должностные лица органов предварительного расследования вынуждены обращаться в негосударственные судебно-экспертные учреждения и на договорной основе проводить необходимые исследования. В этой связи перед субъектами расследования возникают трудности, поскольку они не в полной мере могут определить компетентность лица, привлекаемого к производству исследования. При этом содержание указанных заключений специалистов (экспертов), основанных на положениях Концепции, изобилует субъективными выводами, что может привести к привлечению лица к уголовной ответственности за невиновное причинение вреда (ст. 5 УК РФ).

По причине отсутствия в системе МВД России необходимых специалистов в правоприменительной практике известны случаи привлечения преподавателей высших учебных заведений в сфере искусства и философии, а также врачей высшей категории для очного участия в оперативно-розыскных мероприятиях в качестве специалистов по исследованию объектов, относящихся к категории порнографических. Однако такая практика нуждается в дополнительной регламентации, поскольку вызывает много вопросов к порядку ее проведения¹.

По-прежнему остается дискуссионным вопрос о том, в каких областях знаний может возникнуть потребность в случае проведения исследований объектов порнографического содержания.

Следственная и судебная практика, а также уголовно-правовая доктрина исходят из того положения, что для решения вопроса об отнесении спорного объекта к категории порнографических необходимо назначение комплексной судебной экспертизы в виду его междисциплинарного характера. Об этом свидетельствует и примечание к статье 242.1 УК РФ.

Нередко обмен этими материалами сопровождается путем осуществления лицами коммуникативных действий в ИТКС, что обуславливает необходимость комплексного междисциплинарного исследования результатов такой деятельности. В таком случае при исследовании объектов порнографического характера важно устанавливать как содержание (семантический анализ), так и направленность (выявления формируемых социальных установок и способов их формирования) таких материалов, что возможно осуществить только в рамках комплексной психолого-лингвистической экспертизы [5, с. 85-86].

Однако, экспертная задача по определению возраста лиц, представленных на исследуемых объектах, в отсутствие указания на него в их речевой деятельности, на наш взгляд, должна решаться специалистом из другой области научного знания. Для этого используется шкала для оценки стадии полового созревания индивида (шкала Таннера)².

Зачастую исследования проводятся в отношении одних и тех же объектов (цифровые фото- и видеонизображения) с порнографическими изображениями несовершеннолетних, содержание которых однозначно свидетельствует о противоправном характере указанных материалов. В этом случае происходит дублирование работы соответствующих

¹ Материалы архивного уголовного дела № 1-302/2013 // Архив Чкаловского района суда г. Екатеринбурга за 2013 год.

² Шкала Таннера / Сайт Эс Класс Вики. [Электронный ресурс] URL: <https://goo-gl.ru/aOTaa>. Дата обращения: 01.12.2020.

специалистов, тогда как учет проведенных ранее исследований (экспертиз) централизованно не ведется.

Кроме того, по преступлениям анализируемого вида существует необходимость в проведении амбулаторной (стационарной) судебной комплексной сексолого-психолого-психиатрической экспертизы подозреваемого (обвиняемого). А отсутствие необходимых специалистов по месту проведения предварительного следствия обуславливает возникновение ситуации, когда правоохранительные органы вынуждены направлять указанных лиц в ФГБУ «Национальный медицинский центр психиатрии и наркологии имени В.П. Серьского» Министерства здравоохранения Российской Федерации, где проводятся данные исследования. При этом длительность этапирования указанных лиц отрицательно сказывается на сроках предварительного следствия [3, с. 28].

Рост объемов информации и распространение средств вычислительной техники приводит к возрастанию нагрузки на специалистов, осуществляющих исследования электронных носителей информации. Это влечет за собой увеличение сроков проведения таких исследований, а также сказывается на сроках предварительного расследования.

Учитывая изложенное, нами предлагаются меры организационно-методического, правового и материально-технического характера, реализация которых будет способствовать более эффективному использованию судебных экспертиз при расследовании преступлений анализируемого вида:

1. Существует потребность в разработке методики исследования порнографических объектов. В ее содержание должны входить лингвистические словари, положения методологий оценивания изображений несовершеннолетних эротического и порнографического характера, разработанных зарубежными странами, а также требования существующих федеральных государственных образовательных стандартов с целью определения круга лиц, обладающих необходимыми знаниями в указанной сфере и привлекаемых для проведения такого исследования.

2. Необходимо рассмотреть вопрос о создании в каждом федеральном округе на базе государственных органов исполнительной власти субъектов Российской Федерации экспертных центров с включением в его состав экспертов наиболее востребованных специальностей. Примером может выступить ГБУ «Московский исследовательский центр», которое на безвозмездной основе проводит наиболее востребованные судебные экспертизы для правоохранительных органов, дислоцированных в г. Москва (компьютерные, лингвистические, психологические и др.).

3. Руководителям федеральных органов исполнительной власти предлагается ежегодно предусматривать в проекте бюджета соответствующие статьи расходов, связанных с приобретением конкретных программно-аппаратных средств и программного обеспечения, удовлетворяющих потребностям конкретного правоохранительного органа, а также затрат на его последующее обслуживание (обновление лицензий).

4. Профильным специалистам необходимо на постоянной основе проходить обучение по программам дополнительного профессионального образования с целью поддержания своих знаний в актуальном состоянии.

5. Предлагается организовать создание информационного массива, содержащего сведения о всех проведенных исследованиях материалов с порнографическими изображениями несовершеннолетних, ведение которого может быть поручено Роскомнадзору по аналогии с реестром проведенных экспертиз информационной продукции. Использование сведений из указанного информационного массива позволит в кратчайшие сроки назначать исследования в тех же экспертных учреждениях, в которых они уже ранее проводились и по ним имеется приговор суда, вступивший в законную силу. Предоставление и получение таких сведений возможно осуществлять в рамках межведомственного электронного взаимодействия. Кроме того, результаты таких исследований целесообразно использовать и для нужд Роскомнадзора при блокировании сайтов с запрещенной информацией.

6. Следует рассмотреть вопрос об изменении существующего порядка проведения амбулаторной (стационарной) судебной комплексной сексолого-психолого-психиатрической экспертизы подозреваемого (обвиняемого), предусмотрев возможность производства таких исследований только после получения необходимых рекомендаций психиатра и клинического психолога. Указанное предложение основывается на проведенном нами исследовании, согласно которому лица, страдающие расстройством сексуального предпочтения (педофилии), составляют не более 10 % от общего числа лиц, совершающих сексуальные посягательства в отношении несовершеннолетних. В связи с этим выделяется диспропорция между количеством сил и средств, затраченных на проведение данного исследования, и полученными результатами.

7. Необходимо последовательно увеличивать штат сотрудников, проводящих исследования электронных носителей информации.

Библиографический список:

1. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. И.А. Клепицкого. 9-е изд. М.: РИОР: ИНФРА-М. 2018. 508 с.
2. Концепция информационной безопасности детей / Сайт Орловской детской библиотеки им М.М. Пришвина. [Электронный ресурс]. Режим доступа: <https://googl.ru/IUIHO>. Дата обращения: 01.12.2020.
3. Методические рекомендации по расследованию преступлений против половой неприкосновенности несовершеннолетних, совершенных посредством глобальной сети «Интернет» / Под ред. А.М. Багмета. М.: Академия Следственного комитета Российской Федерации. 2016. С. 28-30.
4. Публичный доклад за 2018 год / Сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. [Электронный ресурс] URL: https://rkn.gov.ru/press/annual_reports. Дата обращения: 01.12.2020.
5. Секераж Т.Н., Кузнецов В.О. Исследование информационных материалов – актуальное направление судебно-экспертной деятельности // Закон. 2019. № 10. С. 80-89.

References:

1. Commentary on the Criminal Code of the Russian Federation (itemized) / Ed. I.A. Klepitsky. 9th ed. M.: RIOR: INFRA-M. 2018. 508 p. (In Russ.).
2. The concept of information security of children / Website of the Oryol's children library by M.M. Prishvin. [Electronic resource] URL: <https://goo-gl.ru/IUIHO>. (accessed: 01.12.2020). (In Russ.)
3. Guidelines for the investigation of crimes against the sexual inviolability of minors committed through the global network «Internet» / Ed. A.M. Bagmet. M.: Academy of the Investigative Committee of the Russian Federation. 2016. P. 28-30. (In Russ.).
4. Public report for 2018 / Website of the Federal Service for Supervision of Communications, Information Technologies and Mass Communications. [Electronic resource] URL: https://rkn.gov.ru/press/annual_reports. (accessed: 01.12.2020). (In Russ.).
5. Sekerage T.N., Kuznetsov V.O. Research of information materials – an actual direction of forensic expert activity // Zakon. 2019. No. 10. P. 80-89. (In Russ.).

K.I. Dorofeev

PROBLEM ASPECTS OF USE OF SPECIAL KNOWLEDGE IN INVESTIGATION OF THE PRODUCTION AND TRAFFICKING OF MATERIALS OR OBJECTS WITH PORNOGRAPHIC IMAGES OF MINORS

The article deals with problematic issues of the organization and use of special knowledge in the investigation of the production and trafficking of materials or objects with pornographic images of minors. Taking into account the study of law enforcement practice, organizational, methodological, legal and material-technical measures are proposed, the implementation of which, in the author's opinion, will contribute to a more effective use of the possibilities of forensic examinations in the investigation of crimes of the analyzed type.

Keywords: special knowledge, forensic examination, materials and objects with pornographic images of minors.

Сведения об авторе:

Дорофеев Кирилл Игоревич, Договорно-правовой департамент МВД России, старший эксперт отдела информационно-правового обеспечения Управления правовой информации.

Адрес электронной почты: moskowlirik@mail.ru

About the author:

Kirill Ig. Dorofeev, Treaty and Law Department of the Ministry of Internal Affairs of the Russian Federation, senior expert of the information and law support unit of the Office of law information.

Email: moskowlirik@mail.ru

СТРАТЕГИЧЕСКИЕ КОММУНИКАЦИИ В ПРОТИВОДЕЙСТВИИ ИДЕОЛОГИИ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В ЭРУ КОРОНАВИРУСА И «ПОСТ-ПРАВДЫ»

ДОРОШЕНКО Е.И.

В статье представлены результаты исследования, проведённого на материале англоязычных источников с целью выявления и определения некоторых особенностей медиапространства, сформировавшихся в условиях пандемии COVID-19. Главным предметом рассмотрения стали идеологические установки исламистских и крайне правых группировок.

Были отмечены неблагоприятные тенденции развития ситуации в информационном поле: идеологи экстремистских и террористических организаций различного толка обращают подавленное эмоциональное состояние и соответствующие запросы аудиторий традиционных и альтернативных СМИ себе на пользу и стремятся как можно активнее продвигать свои тезисы. Как правило, предлагаются объяснения происходящему, назначаются виновные («враги») и даётся вполне конкретный ответ на вопрос о том, что делать и как жить дальше, сформулированный как призыв к определённым деструктивным действиям. На фоне пандемии коронавируса повышенная восприимчивость общественности, в частности молодёжи «поколения Z», к подобным идеологическим выкладкам объясняется, с одной стороны, тревожностью и неуверенностью в завтрашнем дне, а с другой – глубоким знанием современных информационных технологий, способностью с лёгкостью находить информацию, соответствующую определённым запросам. При этом такие качества информации как объективность, точность и правдивость перестают быть значимыми, истолкования (мнения) преобладают над фактами.

В качестве возможного пути преодоления данной ситуации в информационном поле и в рамках противодействия деструктивным идеологиям предлагается шире использовать стратегические коммуникации, в частности нарративы, как наиболее действенное и психологически приемлемое средство.

Ключевые слова: СМИ, медиапространство, «пост-правда», идеология, экстремизм, терроризм, «поколение Z», противодействие, стратегические коммуникации, нарративы.

Тема данной статьи была выбрана неслучайно: пандемия COVID-19 стала, без преувеличения, главным событием 2020 года. Сложившаяся ситуация так или иначе затронула каждого, при этом привычные условия жизни общества существенно – а в некоторых случаях и радикально – изменились. Информационное пространство также испытало на себе влияние этих перемен: это отразилось, в первую очередь, на характере и содержании материалов, которые пользуются наибольшим спросом у аудиторий и традиционных, и альтернативных СМИ.

С целью выявить главные особенности и направления происходящих изменений, автор провёл исследование, в основу которого были положены материалы конференции «Национальная безопасность, фэйк-ньюс и стратегические коммуникации в цифровую эпоху» Тель-Авивского Института исследований национальной безопасности (INSS),

проходившей в ноябре 2020 года, а также тезисы научных проектов разных лет американской корпорации RAND.

Характеризуя современное состояние информационного пространства, Майкл Рич, президент и генеральный директор корпорации RAND, руководящий проектом Truth Decay, выделяет 4 основные тенденции, свидетельствующие о таком явлении, как «упадок правды» [1]:

- 1) Всё более значительные расхождения в интерпретации объективных данных и фактов;
- 2) Размывание границ между фактом и мнением;
- 3) Намечающееся преобладание мнений над фактами: более быстрый количественный рост информации, которую можно отнести к «мнениям» - а значит, и более значительное их влияние – по сравнению с фактами;
- 4) Снижение доверия к учреждениям, которые ранее считались признанными источниками объективных фактов и данных.

Более того, уход от фактов и отмеченное смещение интереса и доверия аудиторий в сторону «мнений» происходит в контексте «эры пост-правды», т.е., по определению Оксфордского словаря, такой политической культуры, где убеждения, ... чувства и эмоции имеют большее влияние [на аудитории], чем факты [2]. Термин вошёл в обиход ещё в 2016 г., в связи с такими событиями, как Brexit и президентские выборы в США.

Всё это может означать, что объективность стала, в каком-то смысле, неинтересна тем, кто находится в медиапространстве: пользователи по-прежнему следят за текущими событиями и занимаются поиском информации, однако такие её качества, как точность и правдивость для них теперь не на первом месте.

В контексте пандемии COVID-19 эти тенденции обозначились ещё резче. В ситуации неопределённости обыватели оказались более склонны искать некую привлекательную картину происходящего, пусть даже не основанную на доказательствах, в соцсетях, а не в официальных источниках.

С одной стороны, это объясняется расхожим убеждением, что «власти всё скрывают», а с другой – желанием найти подтверждение собственному мнению, пусть и субъективному. Этому также способствует уже сложившийся к данному моменту статус соцсетей как «социальных СМИ», а блогеров – как независимых гражданских журналистов, которые находятся непосредственно на месте событий и не связаны обязательствами перед редакторами. Другими словами, аудиториям нужны объяснения (по возможности, интересные), что происходит и указания, что делать – как жить – дальше, пусть даже и ничем не подтверждённые.

В таких условиях и при наличии вышеупомянутого пользовательского запроса в медиапространстве происходит активизация как радикальных исламистских, так и крайне правых (расистских, неофашистских) группировок. И те, и другие выстраивают свою аргументацию, предлагая, в первую очередь, ответ на вопрос «кто виноват»: некий враг теперь несёт ответственность не только за абстрактное несовершенство мира (почему мы – т.е. определённый группировкой круг «своих» – так плохо живём), но и за конкретные

проблемы – тяжёлую болезнь и безработицу. Одни обвиняют «крестоносцев», которые навлекли своим безбожием на себя и весь мир вполне материальную «кару небесную», другие – мигрантов, которые «завезли инфекцию» и, конечно, жителей Восточной и Юго-Восточной Азии за то, что коронавирус там появился.

Соответственно, отвечая на следующий вопрос – «что делать» – и те, и другие сходятся во мнении, что нужно изменить политический строй.

Исламисты – в частности, идеологи запрещённого в России ИГ – настаивают на воссоздании своего псевдохалифата, где всё будет выстроено в соответствии с законами Всевышнего и поэтому шансов на спасение (прежде всего, духовное) больше. Крайне правые радикалы, в свою очередь, предлагают видение «чистого» мира без «иных», от которых «все проблемы».

Поскольку медиапространство активно наполняется подобными выкладками, а обыватель, как было отмечено выше, психологически стремится к оригинальным, а не к объективно-научным поискам выхода, обостряется проблема вербовки в экстремистские и террористические организации. При этом особенно уязвимыми в этом отношении оказываются представители так называемого «поколения Z» – молодые люди, родившиеся в период между 1997 и 2012 годами. Авторы исследования корпорации RAND, посвящённого молодёжи в рядах салафитов-джихадистов, видят «поколение Z» следующим образом [3]:

- Представители «поколения Z» (т.е. люди, родившиеся в период с 1997 по 2012 годы) отличаются «исключительно глубоким знанием технологий, что... оказывает значительное влияние на их взаимодействие с обществом, когнитивные способности, психологическое развитие и мировоззрение.

- ...[Кроме того, поскольку их социо-эмоциональные реакции всё ещё] находятся в стадии формирования, эти молодые люди оказываются более восприимчивы к сенсационным материалам, вызывающим эмоциональный отклик и обещающим быстрое вознаграждение, а также [более склонны] к [действиям], связанным с риском – к протестам или насилию».

Одним из возможных способов преодоления складывающейся неблагоприятной ситуации в медиапространстве является применение стратегических коммуникаций.

Они определяются следующим образом [4]:

Стратегические коммуникации – это согласованные действия, сообщения, изображения и всё, что имеет целью информировать, оказать воздействие или убедить определённые аудитории в поддержку государственных целей.

Сюда входят и связи с общественностью, и народная дипломатия, и информационно-психологическое воздействие – в частности, пропаганда, информационные операции и психологические операции.

В более общем смысле – по определению экспертов Лондонского Королевского колледжа – стратегические коммуникации представляют собой совокупность способов влияния на формирование и изменение значимого политического и геополитического

дискурса в долгосрочной перспективе [5]. Таким образом, «влияние» оказывается ключевым компонентом для обоих определений.

Одним из инструментов стратегических коммуникаций являются нарративы. В терминах филологии они ассоциируются с понятиями «повествования», «рассказа». В более распространённом, ненаучном значении их можно определить как трактовки, истолкования, авторские интерпретации и версии событий, а также линии (углы) подачи информации, а с точки зрения безопасности – это установки, при помощи которых на аудиторию может быть оказано значительное информационно-психологическое воздействие.

Нарративы оформляются, прежде всего, как лингвистические конструкции, которые могут быть дополнены невербальными, как правило, визуальными средствами в целях усиления эффекта. Кроме того, воздействие нарративов может быть усилено и некоторыми другими методами, такими как использование удачных формулировок, структурированная и логичная подача информации в сообщениях (в частности, определённым образом выстроенная последовательность тезисов), применение выразительных и качественных иллюстраций и видео, общая ориентация на определённые ожидания и особенности восприятия целевой аудитории при подготовке материалов.

Таким образом, вышеупомянутый интерес аудиторий к ярким и оригинальным информационным картинкам (при условии, что критерий объективности оказывается не столь значим), можно использовать для создания и распространения позитивного контента, в котором приводились бы объективные факты и данные. Другими словами, создав нарративы более качественные (в том числе и в терминах правдивости и объективности) и привлекательные – по сравнению с экстремистской и террористической пропагандой – и применив их в информационном пространстве, можно было бы скомпенсировать рост и удельный вес негативного контента и попытаться нейтрализовать эффект вербовочных призывов.

В отличие от соцсетевых механизмов мобилизации, которые всё же нельзя считать надёжным рецептом, применимым в любом ситуационном контексте, даже если они некогда отлично сработали, нарративы более стабильны и универсальны, поскольку основаны на более древних психологических особенностях человека – любви к повествованиям.

При этом, занимаясь исследованиями в этом направлении, следует избегать излишней ориентации на политику, иначе возникает риск оказаться в плену того или иного нарратива в ущерб научной объективности. Так, например, наши западные партнёры сегодня всецело сосредоточены на противодействии – в том числе и при помощи стратегических коммуникаций – предполагаемому вмешательству России в американские выборы во имя глобальной и всеобщей демократии (т.е. даже не для того, чтобы защитить и сохранить конкретный государственный строй).

Работая с террористическим и экстремистским контентом, занимаясь поисками эффективных способов профилактики и противодействия, следует помнить, что в этом случае угроза гораздо более реальна и осязаема, чем пресловутые «кремлёвские тролли».

Библиографический список/ References:

1. INSS Annual Conference National Security, Fake News and Strategic Communications in the Digital Era: [Electronic resource] URL: https://www.youtube.com/watch?v=jqKPwJTASrg&feature=emb_logo, 1:48 – 15:00 (accessed: 01.12.2020).
2. Ibidem, Panel 1 Disinformation in 2020: Actors, Threats, Solutions [Electronic resource] URL: <https://www.youtube.com/watch?v=XtDItgVxNXY>, 0:37 – 1:00 (accessed: 01.12.2020).
3. Bafta, R.C., Vest, N., Chan, W.Y., Fanlo, A. Defining and Understanding the Next Generation of Salafi-Jihadists // RAND Corporation, August 2019 [Electronic resource] URL: https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE341/RAND_PE341.pdf (accessed: 01.12.2020).
4. Paul, C. Getting Better at Strategic Communication // RAND Corporation, 12.07.2011 [Electronic resource] URL: https://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT366.pdf (accessed: 01.12.2020).
5. [Electronic resource] URL: <https://www.youtube.com/watch?v=XtDItgVxNXY>, 2:02-2:13 (accessed: 01.12.2020).

Elena Ig. Doroshenko

**APPLYING STRATEGIC COMMUNICATIONS IN COUNTERING VIOLENT
EXTREMIST AND TERRORIST IDEOLOGY IN THE ERA OF POST-TRUTH AND
CORONAVIRUS**

The article presents the results of the research aimed at defining certain traits of the media landscape formed under the influence of the COVID-19 pandemic. The study was based on English-language sources; its main subject is the jihadi and far-right ideologies. The author marks adverse developments in the information field, namely, violent extremist and terrorist ideologists make use of the overall depressed state and corresponding demands of the traditional and alternative media users and do their best to promote their narratives. As a rule, they offer explanations to what is happening, point to the “enemy,” and give a very concrete answer to the question, what to do and how to live, usually expressed as a call to specific destructive actions.

Taken against the background of the coronavirus pandemic, the audiences’ increased receptiveness to such statements is based, on the one hand, on the anxiety and uncertainty and, on the other hand, on the advanced technological skills of the younger generation, enabling them to find the information to suit their demands and interests. Simultaneously, such information quality traits as accuracy, objectivity, and fairness lose their significance and interpretations and opinions seem to dominate over facts.

To overcome such an unfavorable situation and counter destructive and violent ideologies, it is suggested to more actively engage strategic communications and counter-narratives, as these information instruments seem to be the most effective and psychologically acceptable.

Keywords: media, media landscape, post-truth, ideology, violent extremism, terrorism, generation Z, countering, strategic communications, narratives.

Сведения об авторе:

Дорошенко Елена Игоревна, Международное информационное агентство (МИА) «Россия сегодня», кандидат филологических наук, выпускающий редактор Отдела общественно-политических проектов Дирекции государственных проектов МИА «Россия сегодня».

Адрес электронной почты: e.doroshenko@rian.ru

About the author:

Elena Ig. Doroshenko, International News Agency Rossiya Segodnya, Candidate of Philology, Copy Editor.

E-mail: e.doroshenko@rian.ru

НЕКОТОРЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИЧЕСКОГО ВЫЯВЛЕНИЯ И ИССЛЕДОВАНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

КАРЕПАНОВ Н.В.

В статье изложены положения о вредоносных программах, существующих уже более четверти века. По статистике наиболее распространены несанкционированные программы враждебного содержания («троянские кони», вирусы, черви, макровирусы). С развитием технического прогресса они только усложняются. Обоснованы суждения о том, что наиболее распространены два направления противодействия таким программам: использование структурно-независимых механизмов; использование структурно-зависимых механизмов. В первом случае устанавливается периодического контроля вычислительной среды. При втором направлении кроме выявления факта воздействия фиксируются и идентифицируются его следы. К решению этой проблемы необходимо подходить комплексно: изучать и оценить обстановку в сетях; осуществить расстановку сил и средств, обеспечение взаимодействия; управлять, планировать и контролировать; координация действий субъектов правоохранительных органов. Важным элементом системы мер борьбы с криминальным использованием вредоносных программ являются меры превентивного характера: правовые; организационно-технические; криминалистические. Кроме того, Интернет-отношения нуждаются в правовом регулировании. Специалисты называют пять направлений такого регулирования: защита личных данных и частной жизни в Сети; регулирование электронной коммерции и иных сделок и обеспечение их безопасности; защита интеллектуальной собственности; борьба против противоправного содержания информации и противоправного поведения в Сети; правовое регулирование электронных сообщений.

Ключевые слова: вредоносные программы, «троянские кони», вирусы, черви, макровирусы, детектирование, антивирусные средства, сканирование; эвристическое сканирование, СЯС-сканирование, антивирусный мониторинг, иммунизация, киберпространство, техническое опережение.

Введение. Вредоносные программы существуют более четверти века. По статистике наиболее распространены несанкционированные программы враждебного содержания («троянские кони», вирусы, черви, макровирусы) [17, с.152-155]. В современном мире множество лабораторий, занимающихся разработкой методов противодействия вредоносным программам («Лаборатория Касперского», «PandaLabs» и другие). Однако снизить активность эксплуатации таких программ не удалось. Более того, с развитием технического прогресса они все более совершенствуются, усложняются [2, с.45-48].

Цель работы. Показать существующие методы противодействия распространению вредоносных программ, снижению их криминального эффекта. В статье показаны перспективы и способы такой борьбы.

Основной материал. В теоретических исследованиях и практической деятельности информационных технологий сложилось два диаметрально противоположных направления противодействий вредоносным программам. Одно из них предполагает независимость

информационных процессов (структурно-независимые механизмы), другое основано на концепции структурно-зависимых механизмов [8, с.176]. Особенностью механизма противодействия в первом случае является установление периодического контроля целостности вычислительной среды, при котором выявляются несанкционированные изменения, вызванные вредоносными программами.

При втором направлении кроме выявления факта воздействия фиксируются и идентифицируются его следы. Сам факт воздействия вредоносной программы тоже устанавливается двухуровневым механизмом контроля информационной системы. В эту систему входит: сравнения текущих результатов выполнения функций обработки информации и функций контроля; сравнения текущих параметров вычислительного процесса с заранее известными эталонными величинами. Каждое такое средство в отдельности обладает ограниченными контролирующими характеристиками. Для правильного принятия решения о наличии вредоносной программы необходим анализ всей совокупности фактов воздействия значимых признаков такого функционирования (трасология воздействия). При этом важным представляется фиксация последовательности всех контрольных точек и вызовов элементов ПО. Тогда можно будет установить время, место, условия и последствия проявления воздействия вредоносной программы.

При структурно-независимых механизмах защиты используются способы детектирования с помощью профессиональных пакетов антивирусных средств. К таким методам относятся: сканирование; эвристическое сканирование; СЯС-сканирование; антивирусный мониторинг; иммунизация [25, с.256].

Сканеры (резидентные и нерезидентные) используются для проверки файлов, секторов и системной памяти для поисков известных и новых (неизвестных сканеру) вирусов. Методы эвристического сканирования предполагают использование алгоритмы анализа статистики последовательности команд. Однако, приложение, использующее данный способ, требует постоянной поддержки. При использовании эвристического анализа контролируются все действия, которые может выполнить проверяемая программа. Посредством данного метода можно обнаружить как вирус, так и сетевого червя, но данный подход также имеет ряд недостатков. Первый заключается в проявлении «ложной тревоги». Кроме того, такой анализ занимает большой отрезок процессорного времени, что не всегда приемлемо. Основным недостатком данного подхода является то, что вредоносная программа выявляется только после выполнения своих задач. Учитывается также и то, что изначально проверяемые приложения устанавливаются из доверительного источника [6, с. 264; 15, с. 758-761].

Некоторые антивирусные средства для обнаружения вредоносных программ реализуют алгоритмы, основанные на подсчете контрольных сумм (СЯС-сумм) для всех хранимых на носителях файлов и системных секторов.

Антивирусные мониторы — это резидентные программы, контролирующие возникновение ситуаций, связанных с функционированием вредоносных программ. В последнее время, благодаря своей надежности, появились антивирусные мониторы, выполненные в виде аппаратных компонентов компьютера. Иммунизаторы — это

программы, имитирующие заражение файлов вредоносными программами. Иммунизаторы делятся на два типа: иммунизаторы, осуществляющие контроль собственного тела, и иммунизаторы, блокирующие заражение определенным типом вредоносной программы. Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение.

Анализ отечественных и зарубежных антивирусных средств показывает, что большинство из такого рода средств используют несколько механизмов детектирования вредоносных программ. Следует отметить, что качественное детектирование в большинстве случаев обеспечивается более новыми антивирусными средствами, базы данных которых имеют, как правило, сигнатуры самых новых вредоносных программ. Анализ типовых ситуаций воздействия вредоносных программ на информационные процессы в защищенных информационных системах позволил установить, что действия вредоносных программ, как специфического вида резидентных компьютерных вирусов файлового типа формально можно представить в виде определенной последовательности действий.

Существо соответствующих этим действиям способов выявления воздействий вредоносных программ заключается в следующем: сравнение последовательности выполняемых контрольных точек; анализ на наличие кодов команд; анализ векторов прерываний. Для контроля выполнения вредоносных функций целесообразно использовать систему контрольных проверок: проверка соответствия данных области значений; проверка предельных значений входных данных.

Особенностью идентификации следов воздействия вредоносных программ является прослеживание через точки вызова программных модулей всей последовательности выполнения информационного процесса во всех контрольных точках. Сами же контрольные точки выбираются исходя из требований достоверности идентификации фактов воздействия вредоносных программ [1, 7, 9, 10, 15, 20, с. 27-30].

Существующие проблемы защиты информационных ресурсов определяются следующими факторами: развитием мировых и национальных компьютерных сетей и новых технологий; переводом информационных ресурсов на электронные носители и концентрацией их в информационных системах; повышением ценности создаваемой и накопленной информации; разработкой и совершенствованием информационных технологий.

Одним из основных условий эффективного противодействия этому виду преступлений является формирование единой системы мер в борьбе с вирусными программами. Практика выявления вредоносных программ убедительно доказывает, что ориентация лишь на технические и технологические средства не имеет значительного успеха. Чем сложнее программно-техническое обеспечение, тем уязвимее средства защиты информации в автоматизированных системах. С развитием информационных технологий всё больший объём информации концентрируется в точках её сбора и обработки. Иерархия контроля позволяет легче обнаружить слабость информационной защиты. Кроме того, система Интернет не имеет административного регулятора, а информация может храниться на Web-сайтах в другой стране или на другом континенте, где законодательство не готово

устанавливать ответственность за хранение и распространение непристойной информации. Проблема должна решаться на международном уровне, возможно в рамках ЮНЕСКО.

Результаты анализа противодействия вредоносным программам позволяют прогнозировать усложнение борьбы с ними ввиду того, что способы совершения воздействий с каждым годом приобретают все более изощренный и трудноопределимый характер. К решению этой проблемы необходимо подходить комплексно. В частности, можно выделить наиболее значимые элементы организации деятельности правоохранительных органов в глобальных информационных сетях: изучение и оценка обстановки в сетях; осуществление оптимальной расстановки сил и средств, обеспечение взаимодействия; управление, планирование и контроль; координация действий субъектов правоохранительных органов [19, с.220].

На наш взгляд, важным элементом системы мер борьбы с криминальным использованием вредоносных программ являются меры превентивного характера. Можно выделить три основные группы предупреждения: правовые; организационно-технические и криминалистические, составляющие в совокупности целостную систему борьбы с этим социально опасным явлением [22, с.74]. Кроме того, думается, что интернет-отношения нуждаются в правовом регулировании. Специалисты называют пять направлений такого регулирования: защита личных данных и частной жизни в Сети; регулирование электронной коммерции и иных сделок и обеспечение их безопасности; защита интеллектуальной собственности; борьба против противоправного содержания информации и противоправного поведения в Сети; правовое регулирование электронных сообщений [18, с. 104-110].

В Интернете пользователь не только получает возможность доступа к различным информационным ресурсам, но и создает канал для доступа к своему компьютеру. Ответственности за помещаемую в Интернет информацию фактически не несет ни автор, ни провайдер. Никто не несет ответственности и за попытки несанкционированного доступа к сетевым информационным ресурсам. Все вопросы защиты собственной информации относятся к компетенции пользователя. Необходима разработка международных правовых положений, устанавливающих ответственность за несанкционированный доступ к ресурсам Интернета. В соответствии с требованиями Резолюции 428 Консультативной Ассамблеи Совета Европы (раздел С) приоритет отдается уважению и защите частной жизни в ущерб праву на свободу информации [11, с. 20].

Стратегия международного сотрудничества в сфере противодействия компьютерной преступности и приоритетные направления ее реализации, в том числе: межгосударственные соглашения, организация межгосударственной оперативно-розыскной деятельности, принятие межгосударственного регламента и совершенствование интеграционных процессов в рамках межгосударственных организаций, обоснование необходимости разработки и принятия соответствующей комплексной межгосударственной программы.

Сопряжено с определенными проблемами в настоящее время и применение судебно-следственными органами методик выявления криминального использования вредоносных

программ, уголовно-правовой нормы об ответственности за их создание, использование и распространение. Пожалуй, главной из них является отсутствие в отечественной доктрине уголовного права единообразного понимания "вредоносной программы" как конструктивного признака ст. 273 Уголовного кодекса Российской Федерации (далее – УК РФ) [5, с. 43-46].

Мы согласны с мнением некоторых ученых, что ключевая проблема, заключается в недостаточной компетентности лиц, занимающихся выявлением и раскрытием криминального использования вредоносных программ. Опросы среди следователей показывают, что 95% респондентов получили юридическое образование. И только 5% обладают еще и образованием по специальности «Информатика и вычислительная техника». 63% опрошенных владеют компьютером на уровне «среднего пользователя», 37% - на уровне «продвинутого пользователя». 79% при этом постигают компьютер самостоятельно, курсы для сотрудников правоохранительных органов посещали только 21%, и незначительный процент (5%) - коммерческие курсы [12, с. 30-33].

Немалые трудности возникают и при проведении осмотра места происшествия, а также при назначении судебных экспертиз. Место происшествия при криминальном использовании вредоносных программ распознается установлением обстановки совершения преступления. Обстановка уголовного правонарушения в этой области деяний, то есть время, пространство и условия, определяется системой киберпространства. Для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания. И начать надо с определения единого понятия киберпространства с точки зрения криминалистики.

Проблемы, связанные с назначением и проведением судебных экспертиз по вопросам криминального использования вредоносных программ в первую очередь, относятся к высокой загруженности экспертов. Следователи, отмечая высокую загруженность государственных судебно-экспертных учреждений, указывают на хроническую несвоевременность выполнения экспертиз. А ведь в 95% случаев проведение экспертизы они поручали государственно-экспертным учреждениям и лишь в 5% - негосударственным [3,4].

Немаловажной проблемой при назначении экспертиз является постановка грамотных вопросов эксперту. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере. Раскрытие и расследование киберпреступлений остается довольно сложной задачей для большинства сотрудников органов предварительного расследования [14, 16, 23, 24]. Это обусловлено целым рядом факторов: отсутствием системных обобщений материалов следственной и судебной практики; недостаточностью методических рекомендаций по организации расследования данного вида преступлений; небольшим опытом работы следователей (отсутствие специализации) с электронно-цифровыми источниками доказательственной информации; недостаточно высоким уровнем подготовки студентов по соответствующей специализации в высших учебных заведениях.

Выводы. Проблемы криминалистического выявления и исследования вредоносных компьютерных программ требуют неотлагательного разрешения. В Первую очередь решить организационные вопросы: повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации следователей (дознателей) по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений. Сложнее в постоянном режиме решать проблемы технического опережения криминальных разработок внедрения вредоносных компьютерных программ, но такую задачу решать также необходимо.

Библиографический список:

1. Антимонов С. Г. Интеллектуальные противостояния по линии фронта Вирус-антивирус // Информация и безопасность: материалы межрегиональной научно-практ. конф. Информация и безопасность. Выпуск 2. Воронеж: ВГТУ, 2002. 98 с.
2. Аткина В. С. Оценка эффективности катастрофоустойчивых решений // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. — 2012. № 6. 120 с.
3. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд.юрид.наук. Ижевск, 2002. 190 с.
4. Букалерева Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... докт. юрид. наук. М., 2007.
5. Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления / В.Б. Вехов // Расследование преступлений: проблемы и пути их решения. 2015. N 2 (8). С.43-46.
6. Завгородний В. И. Комплексная защита информации в компьютерных системах. — Москва «Логос», 2001. 264 с.
7. Касперски К. Техника сетевых атак. Приемы противодействия. М.: Солон-Р, 2001. 397 с.
8. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью /В. Е. Козлов. М.: Горячая линия - Телеком, 2002. 176 с.
9. Киселев В. В., Ярош В.А. Противодействие вредоносным программам: способы и средства. 2020. 89 с.
10. Лозинский Д. Н. Информационная безопасность. Проблема нового тысячелетия / Д. Н. Лозинский, Е.В. Плескач // Системы безопасности. 2002. № 4(46).
11. Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Автореферат дис. ...д-ра юрид. наук. М.: 2006.
12. Лузгин И. И. Техничко-криминалистическое обеспечение как мегаинструментальная технология формирования единого криминалистического пространства // Эксперт-криминалист. 2010. N 1. С. 30-33.

13. Лысенко, А. В. Анализ методов обнаружения вредоносных программ / А. В. Лысенко, И. С. Кожевникова, Е. В. Ананьин, А. В. Никишова. // Молодой ученый. 2016. № 21 (125). С. 758-761.

14. Лысов Н. Н., Салтевский М.В. Новый подход в технологии собирания и исследования информационных следов // Эксперт-криминалист. 2008. N 1. С. 16-19.

15. Минаев В. А. Принципы организации противодействия вредоносным программам в информационно-телекоммуникационных системах на основе оптимизации их функционирования / В. А. Минаев, С.В. Скрыль // Радиосистемы. Вып. 47 «Радиотехнические и информационные системы охраны и безопасности». Радиотехника. 2000. №9. С. 71-72.

16. Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: дис. ... канд. юрид. наук. Краснодар, 2009.

17. Никишова А. В. Программный комплекс обнаружения атак на основе анализа данных реестра // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. 2012. № 6. С.152-155.

18. Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Сборник научных трудов международной конференции “Информационные технологии и безопасность”. Выпуск 3. Киев: Национальная академия наук Украины, 2003. С.104-110.

19. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. М.: Норма, 2004. 320 с.

20. Распределенный антивирусный контроль как способ противодействия вредоносным программам в автоматизированных информационных системах / С. В. Скрыль и др. // Радиосистемы. Вып. 37 «Радиотехнические и информационные системы охраны и безопасности». Радиотехника. 1999. №6. С. 27-30.

21. Сердюк В.А. Перспективные технологии обнаружения информационных атак / В.А. Сердюк // Системы безопасности. 2002. № 5 (47). С.96-97.

22. Старостина Е. В., Фролов Д. Б. Защита от компьютерных преступлений и кибертерроризма. М.: Изд-во Эксмо, 2005.

23. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. ... канд. юрид. наук. М., 2005.

24. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток, 2005.

25. Фролов А. В., Фролов Г. В. Осторожно: компьютерные вирусы. М.: ДИАЛОГ-МИФИ, 1996. 256 с.

References:

1. Antimons S.G. Intelligent Confrontations on the front-line Virus-antivirus // Information and security: materials of interregional scientific and practical. Conf. Information and security. Issue 2. Voronezh: VGTU, 2002. 98 p. (In Russ.)

2. Atkina V.S. Assessment of the effectiveness of disaster-resistant solutions // Herald of Volgograd State University. Episode 10. Innovation. 2012. No 6. 120 p. (In Russ.)

3. Brazhnik S.D. Crimes in the field of computer information: problems of legislative technology: dis. ... Candidate of Sciences (Law). Izhevsk, 2002. 190 p. (In Russ.)
4. Bukalerova L.A. Information crimes in the sphere of state and municipal government: law-making and law enforcement problems: dis. ... Dr. of Sciences (Law). M., 2007. (In Russ.)
5. Vekhov V.B. Malware computer programs as an object and a means of committing a crime // Investigation of crimes: problems and ways to solve them. 2015. N 2 (8). P. 43-46. (In Russ.)
6. Zavgorodniy V.I. Comprehensive protection of information in computer systems. Logos Moscow, 2001. 264 p. (In Russ.)
7. Kaspersky C. Network Attack Technique. Countermeasures. M.: Solon-R, 2001. 397 p. (In Russ.)
8. Kozlov V.E. Theory and practice of combating computer crime / V.E. Kozlov. M.: Hotline-Telecom, 2002. 176 p. (In Russ.)
9. Kiselyov V., Yarosh V.A. Anti-Malware: Ways and Means. 2020. 89 p.
10. Lozinski D. N. Information Security. The problem of the new millennium / D.N. Lozinski, E.V. Pleskac // Security Systems. 2002. No 4(46). (In Russ.)
11. Lopatina T. M. Criminological and Criminal-Legal Frameworks for Countering Computer Crime. Abstract dis. ... Dr. of Sciences (Law). M.: 2006. (In Russ.)
12. Luzgin I. I. Technical-criminal support as a mega-instrumental technology of the formation of a single forensic space // Forensic expert. 2010. N 1. P. 30-33. (In Russ.)
13. Lysenko A.V. Analysis of malware detection methods / A.V. Lysenko, I.S. Kozhevnikova, E.V. Ananyin, A.V. Nikishova. // Young scientist. 2016. No 21 (125). P. 758-761. (In Russ.)
14. Lysov N., Saltevsy M.V. A new approach in the technology of collecting and researching information traces / Forensic expert. 2008. N 1. P.16-19. (In Russ.)
15. Minaev VA Principles of organization of anti-malware programs in information and telecommunications systems by optimizing their functioning / V.A. Minaev, S.V. Snwing // Radiosystems. "Radiotechnical and Information Systems for Security and Security." Radio equipment. 2000. No9. P. 71-72. (In Russ.)
16. Narizhny A.V. Use of special knowledge in the detection and investigation of crimes in the field of computer information and high technology: dis. ... Candidate of Sciences (Law). Krasnodar, 2009. (In Russ.)
17. Nikishova A.V. Attack Detection Program complex based on the analysis of registry data // Volgograd State University Gazette. Episode 10. Innovation. 2012. No 6. P.152-155. (In Russ.)
1. Nomokonov V.A. Topical Problems to Combat Cybercrime / A collection of scientific papers of the international conference "Information Technology and Security." Issue 3. - Kiev: National Academy of Sciences of Ukraine, 2003. P. 104-110. (In Russ.)
2. Osipenko A.L. Fighting Crime in Global Computer Networks: International Experience: Monograph. M.: Norma, 2004. 320 p. (In Russ.)

18. Distributed antivirus control as a way to counteract malware in automated information systems / S.V. Skri'l, etc. // Radio systems. You are going to drink. 37 "Radiotechnical and Information Systems for Security and Security". Radio equipment. 1999.

3. Serdyuk V.A. Advanced Information Attack Detection Technology / V.A. Serdyuk // Security Systems. 2002. No 5(47). P.96-97. (In Russ.)

4. Starostina E.V., Frolov D.B. Protection from computer crimes and cyberterrorism. M.: Exmo, 2005. P.74. (In Russ.)

19. Stepanov-Yegiants V.G. Crimes in the field of security circulation of computer information: comparative analysis: dis. ... Candidate of Sciences (Law). M., 2005.

5. Tropina T.L. Cybercrime: Concept, State, Criminal Action: Dis. ... Candidate of Sciences (Law). Vladivostok, 2005. (In Russ.)

20. Frolov A.V., Frolov G. V. Beware: computer viruses. -M.: DIALOGUE-MIFI, 1996. 256 p. (In Russ.)

Nikolai V. Karepanov

SOME PROBLEMS OF FORENSIC DETECTION AND RESEARCH OF MALICIOUS COMPUTER PROGRAMS

The article outlines the provisions for the bearers (malicious program) programs that have existed for more than a quarter of a century. With the development of technological progress, they only become more complex. The two areas of resistance to such programs are the most common: the use of structurally independent mechanisms of on; the use of structural-dependent mechanisms. The solution to this problem needs to be addressed comprehensively: to study and evaluate the situation in the networks; to implement and balance the forces and means, to ensure cooperation; to manage, plan and control; coordination of actions of law enforcement actors. Forensic. In addition, Internet relationships need to be regulated.

Keywords: inbred-bearing programs, Trojan horses, viruses, worms, macro viruses, detections, antivirals and, scanning; heuristic scanning, ALL scanning, antivirus monitoring, immunization, cyberspace, technically ahead.

Сведения об авторе:

Карепанов Николай Васильевич, Уральский государственный юридический университет (Екатеринбург), доцент кафедры криминалистики, кандидат юридических наук.

Адрес электронной почты: karepanovvv@gmail.com

About the author:

Nikolai V. Karepanov, Ural State Law University (Yekaterinburg), Associate professor of the Department of criminalistics, Candidate of Science (Law).

E-mail: karepanovvv@gmail.com

О ПРОПАГАНДЕ НАРКОТИЧЕСКИХ СРЕДСТВ В СЕТИ ИНТЕРНЕТ В АСПЕКТЕ СУДЕБНОЙ ЛИНГВИСТИЧЕСКОЙ ЭКСПЕРТИЗЫ

ЛЕБЕДЕВА А.К.

Статья посвящена некоторым аспектам производства судебной лингвистической экспертизы по делам о пропаганде наркотиков в сети Интернет. Подчеркивается важность данной темы в современном обществе. Острый характер данная проблема приобретает в свете недавних поручений Президента России Владимира Путина о подготовке поправок «о введении уголовной ответственности за пропаганду или склонение к употреблению наркотиков в интернете». Особое внимание уделено проблеме определения понятия «пропаганда», объема данного понятия, несоответствия законодательной формулировки понятия «пропаганда наркотических средств» и понятия «пропаганда» в лингвистическом понимании.

Ключевые слова: судебная лингвистическая экспертиза, судебная экспертиза, пропаганда наркотических средств, Интернет.

Ежегодно правоохранительными органами выявляется около 200 тысяч преступлений, связанных с незаконным оборотом наркотиков¹. На данную статистику влияет и активная пропаганда наркотических средств, осуществляемая в сети Интернет. Пропаганда наркотических средств на такой быстро развивающейся и открытой площадке, как Интернет, безусловно может воздействовать на аудиторию, способствовать вовлечению новых лиц, в том числе и несовершеннолетних, в незаконный оборот наркотических средств. Таким образом, в современных реалиях пропаганда наркотических средств в сети Интернет является информационной угрозой, которой лица, обладающие специальными знаниями, должны противодействовать.

Острый характер данной проблемы подчеркивается неоднократными высказываниями Президента Российской Федерации на эту тему. Не так давно средства массовой информации активно освещали поручения Президента России Владимира Путина о подготовке поправок «о введении уголовной ответственности за пропаганду или склонение к употреблению наркотиков в интернете»², которые были сформулированы по результатам встречи с представителями общественности Дальнего Востока от 25.10.2019: «внесение в законодательство Российской Федерации изменений, устанавливающих уголовную ответственность за склонение к потреблению либо пропаганду наркотических

¹ Указ Президента Российской Федерации от 23.11.2020 № 733 "Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года". [Электронный ресурс] URL: <http://publication.pravo.gov.ru/Document/View/0001202011230073?index=6&rangeSize=1> (дата обращения: 25.11.2020 г.)

² [Электронный ресурс] URL: <https://tass.ru/obschestvo/7052374> (дата обращения: 25.11.2020 г.)

средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационной сети Интернет» (п.8. ч.2.)¹.

23 ноября 2020 года указом президента Российской Федерации была утверждена стратегия государственной антинаркотической политики России на период до 2030 года. В указанной стратегии как раз подчеркивается угроза национальной безопасности страны: «Масштабное использование сети «Интернет» для пропаганды незаконного потребления наркотиков»².

С одной стороны, мы понимаем, что некоторые ужесточения в сфере контроля за распространением противоправной информации в сети Интернет просто необходимы, с другой стороны, ведутся оживленные споры о формулировке понятия «пропаганда наркотических средств», и как следствие это приводит к волнениям и обеспокоенности правозащитных организаций, юристов, экспертного сообщества.

В настоящее время ответственность за пропаганду либо незаконную рекламу наркотических средств, психотропных веществ или их прекурсоров закреплена в статье 6.13 КоАП РФ. В указанной статье понятие «пропаганда наркотических средств» не раскрывается, однако оно закреплено в ФЗ «О наркотических средствах и психотропных веществах» в статье 46:

«1. Пропаганда наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, культивирования наркосодержащих растений, осуществляемая юридическими или физическими лицами и направленная на распространение сведений о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений, а также производство и распространение книжной продукции, продукции средств массовой информации, распространение указанных сведений посредством использования информационно-телекоммуникационных сетей или совершение иных действий в этих целях запрещаются.

2. Запрещается пропаганда каких-либо преимуществ в использовании отдельных наркотических средств, психотропных веществ, их аналогов или прекурсоров, новых потенциально опасных психоактивных веществ, наркосодержащих растений, в том числе пропаганда использования в медицинских целях наркотических средств, психотропных веществ, новых потенциально опасных психоактивных веществ, наркосодержащих растений, подавляющих волю человека либо отрицательно влияющих на его психическое или физическое здоровье»³.

Однако если сравнить данное в законе определение со словарным значением слова «пропаганда», то видно, что значения разнятся.

¹ Перечень поручений по итогам встречи с представителями общественности Дальнего Востока от 25.10.2019 // Официальный сайт Президента Российской Федерации. URL <http://kremlin.ru/assignments/orders/61916> (Дата обращения 25.11.2020)

² Указ Президента Российской Федерации от 23.11.2020 № 733 "Об утверждении Стратегии государственной антинаркотической политики Российской Федерации...».

³ Федеральный закон от 08.01.1998 N 3-ФЗ (последняя редакция) "О наркотических средствах и психотропных веществах" // СПС «Консультант-плюс»

Например, в Современном толковом словаре русского языка понятие «пропаганда» определено следующим образом: «Распространение в обществе каких-либо идей, воззрений, знаний путем постоянного глубокого и детального их разъяснения» [6].

Профессор Е.И. Галяшина определяет понятие пропаганды следующим образом: «деятельность, направленная на то, чтобы повлиять на сознание индивидов, отдельных общественных групп или на общество в целом для достижения определенной, заранее намеченной цели» [1, с.15].

Указанные определения сходятся в том, что пропаганда всегда связана с распространением информации, однако в действующем законодательстве, в определении понятия «пропаганда наркотических средств» отсутствует указание на цели ее распространения. По сути, законодательное определение запрещает распространение определенной информации, что само по себе пропагандой не является. Пропаганда всегда связана с воздействием на аудиторию, убеждением её в принятии определенных взглядов.

По данной категории дел часто для установления факта пропаганды возникает необходимость в использовании специальных знаний. В связи с тем, что объектом исследования является в большинстве случаев продукт речевой деятельности с зафиксированными «речевыми следами», то, как пишет Е.И. Галяшина, «без проведения лингвистической экспертизы невозможно установить сам факт пропаганды наркотических средств и привлечь нарушителя к ответственности» [2]. Соответственно, вопрос об установлении диагностического комплекса лингвистических признаков пропаганды активно обсуждается в специальной литературе.

Объектами судебной лингвистической экспертизы по делам о пропаганде наркотиков могут быть как просто тексты различного объема (статьи в СМИ, блоги, посты в социальных сетях), креолизованные тексты (мемы, посты в Инстаграм, иных социальных сетях), аудиовизуальные произведения (публикации на видеохостинге Youtube и т.д.) фонограммы песен различных исполнителей.

Пропаганда как речевое действие без привязки именно к лексико-семантическому полю «наркотики» рассматривалась в различных работах [см., например, 4, 5]. Еще в 2006 году была разработана методические рекомендации для проведения лингвистической экспертизы текстов, в которых имеется информация, относящаяся к семантическому полю «наркотики» [3]. Тем не менее, единый научно-методический подход к установлению лингвистических признаков пропаганды не выработан.

Нередко объектами судебно-экспертного лингвистического исследования становятся различные дневниковые записи, содержащие рассказы лиц о личном негативном опыте употребления наркотических средств, зависимости от них, способов излечения от данной зависимости: «Три года безумия на острие иглы... Поначалу кайф, но потом понимаешь, что не кайф, а кабала. «Я себя контролирую», — стандартные слова, которыми можно просто себя обманывать, потому что никакого контроля нет с самого первого дня...»¹. Подобные речевые произведения могут содержать в том числе и информацию о способах

¹ Электронный ресурс URL: <https://psychologyc.ru/dnevnik-narkomana/> (Дата обращения 25.11.2020)

использования наркотиков с разной степенью детализации. При их анализе важно обращать внимание на речевые цели, выраженные в тексте, действительно ли целью автора является пропаганда наркотических средств, а не демонстрация личных переживаний и предупреждение лиц о негативном воздействии наркотических средств на организм, предостережение от возможного употребления запрещенных веществ в будущем. Наличие в речевом произведении только информации о наркотических веществах, способе их употребления не может быть отнесено именно к пропагандистскому дискурсу.

Кроме того, особую дискуссию вызывают вопросы, связанные с обсуждением вопроса о легализации «легких» наркотиков. Возможность подобных дискуссий в целом, так и просто использования определения «легкий» по отношению к наркотикам возникает вследствие неоднозначной мировой практики: снятие запрета на продажу и употребление отдельных видов наркотиков в некоторых странах. В случае анализа текстов на подобную тематику также необходимо лингвистически доказать пропагандистский характер такого речевого продукта.

Принимая во внимание вышесказанное, как законодательные формулировки, так и понятийно-терминологический аппарат судебной лингвистической экспертизы необходимо пересмотреть в целях выработки единообразного понимания и применения термина «пропаганда наркотических средств».

Библиографический список:

1. Галяшина Е.И. К вопросу об установлении факта пропаганды наркотиков // Профилактика немедицинского потребления наркотических средств и психотропных веществ: проблемы и пути решения: Материалы Всероссийской научно-практической конференции с международным участием. ИП Киселев А. В. Вологда, 2017. С.13-19.
2. Галяшина Е.И. Лингвистическая безопасность речевой коммуникации. URL <http://filfak.mrsu.ru/shigurov/galash.html>. (Дата обращения 25.11.2020 г.)
3. Голощапова Т.И., Смирнов А.А., Полосина А.М., Курьянова И.В. / Под редакцией д.ю.н., профессора А.М. Черенкова. Лингвистическая экспертиза текстов, в которых имеется информация, относящаяся к семантическому полю «наркотики»: методические рекомендации для экспертов, следователей, оперативных сотрудников. – М.: ЭКУ 9 Департамента Федеральной службы Российской Федерации по контролю за оборотом наркотиков, 2006 г. 43 с.
4. Кукушкина О.В., Сафонова Ю.А., Секераж Т.Н. Методика проведения судебной психолого-лингвистической экспертизы материалов по делам, связанным с противодействием экстремизму и терроризму. М.: ФБУ РФЦСЭ при Минюсте России, 2014. 98 с.
5. Никишин В.Д. Теоретические и организационно-правовые аспекты судебной экспертизы материалов религиозного характера экстремистской и террористической направленности: дис. ... канд. юрид. наук: 12.00.12 / Никишин Владимир Дмитриевич. - М., 2019. 276 с.
6. Современный толковый словарь русского языка Т.Ф. Ефремовой. М.: Русский язык, 2011.

References:

6. Galyashina E.I. On the issue of establishing the fact of drug propaganda // Prevention of non-medical consumption of narcotic drugs and psychotropic substances: problems and solutions: Materials of the All-Russian scientific and practical conference with international participation. IP Kiselev A.V. Vologda, 2017. P.13-19. (In Russ.)
7. Galyashina E.I. Linguistic safety of speech communication. URL <http://filfak.mrsu.ru/shigurov/galash.html>. (Date of treatment 11/25/2020). (In Russ.)
8. Goloshchapova T.I., Smirnov A.A., Polosina A.M., Kuryanova I.V. / Edited by Doctor of Law, Professor A.M. Cherenkov. Linguistic examination of texts containing information related to the semantic field of "drugs": guidelines for experts, investigators, operational staff. - M.: ECU 9 of the Department of the Federal Service of the Russian Federation for Drug Control, 2006. 43 p. (In Russ.)
9. Kukushkina O.V., Safonova Yu.A., Sekerazh T.N. Methods of conducting a forensic psychological and linguistic examination of materials in cases related to countering extremism and terrorism. Moscow: FBU RFTsSE under the Ministry of Justice of Russia, 2014. 98 p. (In Russ.)
10. Nikishin V.D. Theoretical and organizational and legal aspects of forensic examination of materials of a religious nature of extremist and terrorist orientation: dis. ... Cand. jurid. Sciences: 12.00.12 / Nikishin Vladimir Dmitrievich. - M., 2019. 276 p. (In Russ.)
11. Modern explanatory dictionary of the Russian language T.F. Efremova (In Russ.)

Antonina K. Lebedeva

ABOUT PROPAGANDA OF NARCOTIC DRUGS ON THE INTERNET IN THE ASPECT OF FORENSIC LINGUISTIC EXPERTISE

The article deals with some problems of the forensic linguistic examination in cases of drug propaganda on the Internet. The importance of this topic in modern society is emphasized. This problem is becoming acute in the light of the recent instructions of Russian President Vladimir Putin on the preparation of amendments "on the introduction of criminal liability for propaganda or inducement to use drugs on the Internet. Particular attention is paid to the problem of the propaganda's definition, the discrepancy between the legislative formulation of the concept of "drug's propaganda" and the concept of propaganda in the linguistic sense.

Keywords: forensic linguistics, forensic science, propaganda of narcotic drugs, Internet.

Сведения об авторе:

Лебедева Антонина Константиновна, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), старший преподаватель кафедры судебных экспертиз, кандидат юридических наук.

ЛЕБЕДЕВА А.К.

Адрес электронной почты: tonya109@yandex.ru

About the author:

Antonina K. Lebedeva, Kutafin Moscow State Law University (MSAL), Senior lecturer of Forensic Expertise's department, Candidate of Science (Law).

E-mail: tonya109@yandex.ru

СОБЛЮДЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ КАК ПРИНЦИП СУДЕБНО-ЭКСПЕРТНОЙ ЭТИКИ

МЫСКИНА К.М.

В статье рассмотрены особенности принципа конфиденциальности информации в деятельности судебного эксперта как одного из основных принципов судебно-экспертной этики. Дан краткий обзор текущего законодательства, освещены проблемы ответственности эксперта за разглашение конфиденциальной информации, проанализирован опыт зарубежных стран. Кроме того, автор поднимает вопрос о необходимости создания единого кодекса судебно-экспертной этики и закрепления в нём принципа конфиденциальности информации.

Ключевые слова: конфиденциальность информации, судебно-экспертная этика, этические принципы, кодекс судебно-экспертной этики.

Понятие этики в научной литературе имеет несколько трактовок. Во-первых, под ним понимают «философское учение о морали, изучающее условия возникновения морали, ее сущность, понятийные и императивные формы» [2]. Как термин, а также научная дисциплина этика восходит ещё к Аристотелю [8]. Нас в большей степени интересует понятие этики в его втором значении: этика – это «система норм нравственного поведения человека, какой-либо общественной или профессиональной группы (например врачебная этика)» [2].

Представители различных профессий нередко сталкиваются с нравственными коллизиями, для решения которых обычных профессиональных знаний недостаточно [3]. Таким образом, возрастает значение профессиональной этики, которая представляет собой конкретизацию общих этических норм.

В настоящее время учёными-правоведами признаётся наличие категории профессиональной этики в юридической профессии, в том числе выделяется этика судебного эксперта, как самостоятельная разновидность судебной этики.

Задачей судебно-экспертной деятельности является оказание содействия судам, следователям, органам дознания и т.д. Судебный эксперт, являясь лицом, обладающим специальными знаниями, назначается в соответствии с процессуальным законодательством судом или следователем для производства судебной экспертизы и дачи заключения [4, с. 130]. Характер его деятельности значительно отличается от деятельности субъектов правоприменения, но имеет не меньшее значение для процесса судопроизводства. Помимо процессуальных различий необходимо отметить, что деятельность судебного эксперта не только является практической познавательной, но носит особый, эвристический характер. Она направлена на получение нового знания на основе уже известного об индивидуально конкретных объектах [4, с. 268].

Результатом экспертного исследования является заключение эксперта. Оно содержит выводы по поставленным перед экспертом вопросам, имеющим значение для производства по делу, и является доказательством во всех видах процесса. Таким образом, вполне

закономерно, что этика судебного эксперта имеет свои особенности по сравнению с судебной этикой.

Очевидно, что процессуальная роль эксперта и его деятельность значительно отличаются от роли и деятельности субъектов правоприменения.

Эти особенности основываются, в том числе, на принципах судебно-экспертной деятельности. В качестве таковых ст. 4 Федерального закона от 31 мая 2001 г. N 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (ФЗ ГСЭД) называет независимость и объективность, а также принцип всесторонности и полноты исследований. Эти же принципы составляют основу судебно-экспертной этики. Значительную роль играют такие категории судебно-экспертной этики, как добросовестности, принципиальности, честности, беспристрастности, стойкости характера, самокритичности, самостоятельности в суждениях и конфиденциальности соблюдения информации. Именно этому, довольно важному с процессуальной точки зрения принципу, мы бы и хотели уделить особое внимание.

Обязанность эксперта соблюдать конфиденциальность информации, полученной в процессе экспертного исследования, закреплена в большинстве процессуальных кодексов и в далее – ФЗ ГСЭД. Так, эксперт не вправе разглашать сведения, которые стали ему известны в связи с проведением экспертизы (п. 5 ч. 4 ст. 57 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ), ч. 2 ст. 85 Гражданско-процессуального кодекса Российской Федерации (далее – ГПК РФ), ч. 6 ст. 49 Кодекса административного судопроизводства (далее – КАС РФ), ст. 16 ФЗ ГСЭД). Кроме того, эксперту запрещено сообщать кому-либо о результатах судебной экспертизы, за исключением органа или лица, ее назначивших (ч. 2 ст. 85 ГПК РФ, ч. 6 ст. 49 КАС РФ, ст. 16 ФЗ ГСЭД).

Указанные законодательные нормы имеют большое значение с точки зрения профессиональной этики судебного эксперта. Эпоха всеобщей цифровизации обязывает уделять особое внимание вопросам отношения эксперта к информации и носителям информации, с которыми ему приходится взаимодействовать в ходе профессиональной деятельности [6, с. 105].

Так, даже в условиях конкуренции для судебно-экспертного учреждения является недопустимым использование информации о проведенных судебных экспертизах в рекламных целях [6, с. 105]. Разглашение подобных сведений – начиная с самого факта проведения экспертизы, и заканчивая её результатами и личными данными участвующих в деле лиц, – может нанести вред как ходу следствия или судебного разбирательства, так и непосредственно лицу, сведения о котором были распространены. Рассматривая данный вопрос, можно усмотреть наличие законодательного пробела. Согласно действующему законодательству, за разглашение данных предварительного расследования эксперт несёт ответственность в соответствии со ст. 310 Уголовного кодекса Российской Федерации. Данное положение содержится в ч. 6 ст. 57 УПК РФ и касается исключительно предварительного расследования. Вопрос, какая санкция следует за разглашение сведений, ставших ему известными в процессе производства судебной экспертизы, не связанных с предварительным расследованием, а также в других видах судопроизводства, в процессуальных кодексах не разрешён. Надо полагать, что подобные действия эксперта

можно расценить как совершение административного правонарушения, предусмотренного ст. 13.14 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ), а именно «разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей».

Не менее важно соблюдение конфиденциальности информации и в тех случаях, когда сотрудники судебно-экспертного учреждения привлекаются к проведению внесудебных исследований в качестве лиц, обладающих специальными знаниями, но не имеющих процессуального статуса.

Ещё одним вопросом, требующим рассмотрения в связи принципом соблюдения конфиденциальности информации, является проблема цифровизации справочно-информационных фондов криминалистического и судебно-экспертного назначения. Современные технологии позволили решить многие проблемы криминалистических учётов путём создания автоматизированных информационно-поисковых систем [5, с. 27]. Актуален вопрос создания базы данных экспертных учреждений по родам и видам экспертиз, которые в них производятся, а также формирования базы данных всех экспертных заключений. Однако эта идея трудно реализуема по ряду причин, связанных в том числе и с судебно-экспертной этикой, в частности, с необходимостью соблюдения принципа конфиденциальности информации [7, с. 136].

О.А. Суровая в своём диссертационном исследовании уделяет внимание вопросам обеспечения конфиденциальности информации в рамках повседневного функционирования судебно-экспертного учреждения. В первую очередь обеспечение защиты конфиденциальных данных лежит на руководителе судебно-экспертного учреждения, который должен определить, как сведения следует относить к конфиденциальной информации, установить правила и способы её безопасной передачи и работы с ней [9, с. 152]. Роль руководителя ни в коей мере не умаляет важности соблюдения принципа конфиденциальности информации рядовыми сотрудниками СЭУ. Так, безопасность информации обеспечивается посредством доведённых до каждого эксперта требований по обращению с конфиденциальной информацией. Мы полагаем, что такие требования должны в должностные инструкции или договоры, на основании которых работают эксперты.

Таким образом, О.А. Суровая выделяет три категории средств, позволяющих обеспечить сохранность конфиденциальной информации: технические средства, (пароли, файрволы, сейфовые хранилища, видеофиксацию рабочих процессов, антивирусные программы); юридические средства и организационные меры [9, с. 152].

Безусловный интерес представляет сравнительный анализ кодексов судебно-экспертной этики зарубежных стран и того, какое место в них отводится принципу соблюдения конфиденциальности информации. Как правило, принцип соблюдения конфиденциальности информации формулируется в подобных документах аналогичным образом, однако мы можем отметить несколько интересных моментов.

Так, Правила профессиональной этики лиц, осуществляющих судебно-экспертную деятельность, Республики Беларусь в рамках регулирования взаимоотношений эксперта с гражданами, отдельно устанавливают, что судебный эксперт не вправе без разрешения граждан разглашать сведения, полученные им в ходе проведения экспертного исследования и составляющие охраняемую законом тайну (ст. 21). Кроме того, интересное положение содержит Кодекс этики судебного эксперта республики Молдовы. Он разрешает использовать материалы, накопленные в ходе судебно-экспертной деятельности, для написания научных статей, но только «после окончательного урегулирования дела» и «с сохранением анонимности в соответствии с законом» (п. 5 ст. 6).

Представляется, что использование такого опыта полезно при создании единого кодекса судебно-экспертной этики в Российской Федерации, в котором, по мнению учёных в области судебной экспертологии, нуждается экспертное сообщество [1]. В рамках подобного Кодекса принцип соблюдения конфиденциальности информации должен быть обозначен в числе основных принципов судебно-экспертной деятельности. Далее необходимо раскрыть его содержания, а также закрепить конкретные санкции за его нарушение.

Библиографический список:

1. Аминев Ф.Г. О профессиональной этике судебного эксперта в Российской Федерации // Электронный научный журнал Байкальского государственного университета, 2016. Т. 7, № 6.
2. Кононенко Б.И. Большой толковый словарь по культурологии. М.: Вече : АСТ, 2003. [Электронный ресурс] URL: https://dic.academic.ru/dic.nsf/enc_culture/2623 (дата обращения 12.01.2021).
3. Малиновский А.А. Кодекс профессиональной этики: понятие и юридическое значение. // Российское законодательства: состояние и проблемы. Журнал Российского права, № 4. 2008 г.
4. Россинская Е.Р., Галяшина Е.И., Зинин А.М. Теория судебной экспертизы (судебная экспертология): учебник. М. : Норма : ИНФРА М, 2017.
5. Россинская Е.Р. Цифровизация справочно-информационных фондов криминалистического и судебно-экспертного назначения как часть учения о цифровизации криминалистической регистрации // Вестник Университета им. О.Е. Кутафина, № 6, 2020. С. 27.
6. Рубис А.С., Кот Я.И. К вопросу о правилах профессиональной этики судебного эксперта // Веснік БДУ. Сер. 3. 2011. No 1.
7. Саркисян А.А. Цифровые базы данных в судебно-экспертной деятельности. Вестник Университета им. О.Е. Кутафина, № 6, 2020.
8. Степин В.С. Новая философская энциклопедия. М.: Мысль, 2000-2001. [Электронный ресурс] URL: https://dic.academic.ru/dic.nsf/enc_philosophy/1436 (Дата обращения 12.01.2021).
9. Суровая О.А. Организационно-правовые аспекты деятельности руководителя судебно-экспертной организации: дис. ... канд. юрид. наук. Москва, 2020. – 210 с.

References:

1. Aminev F.G. On the professional ethics of a forensic expert in the Russian Federation // Electronic scientific journal of the Baikal state University, 2016. Vol. 7, No. 6.
2. Kononenko B.I. The Big Explanatory Dictionary of Cultural Studies. M.: Veche: AST, 2003. [Электронный ресурс] URL: https://dic.academic.ru/dic.nsf/enc_culture/262 (Date of treatment 01/12/2021).
3. Malinovsky A.A. Code of professional ethics: concept and legal meaning. // Russian legislation: state and problems. Journal of Russian Law, No. 4. 2008.
4. Rossinskaya E.R., Galyashina E.I., Zinin A.M. Theory of forensic examination (forensic expertise): textbook. M.: Norma: INFRA M, 2017.
5. Rossinskaya E.R. Digitalization of reference and information funds of forensic and forensic-expert purpose as part of the doctrine of digitalization of forensic registration / / Vestnik Universiteta im. o. E. Kutafin, No. 6, 2020. P. 27.
6. Rubis A. S., Kot Ya. I. To the question of the rules of professional ethics of a forensic expert // Vesnik BDU. Ser. 3. 2011. No 1. P. 105.
7. Sarkisyan A. A. Digital databases in forensic activity. Bulletin of the Kutafin University, No. 6, 2020.
8. Stepin V.S. New philosophical encyclopedia. M.: Thought, 2000-2001. [Электронный ресурс] URL: https://dic.academic.ru/dic.nsf/enc_philosophy/1436 (Date of treatment 01/12/2021).
9. Surovaya O.A. Organizational and legal aspects of the activity of the head of the forensic organization: dis. ... Cand. Sciences (Law). Moscow, 2020. - 210 p.

Kseniya M. Myskina

**MODERN TRENDS IN THE INSPECTION, SEIZURE AND RETRIEVE
INFORMATION FROM THE CARRIERS OF THE DIGITAL INFORMATION**

Abstract. The article discusses the features of the principle of confidentiality of information in the activities of a forensic expert as one of the main principles of forensic expert ethics. A brief overview of the current legislation is given, the problems of expert responsibility for disclosure of confidential information are highlighted, and the experience of foreign countries is analyzed. In addition, the author raises the question of the need to create a unified code of forensic ethics and consolidate the principle of confidentiality of information in it.

Keywords: confidentiality of information, forensic ethics, ethical principles, code of forensic ethics.

МЫСКИНА К.М.

Сведения об авторе:

Мыскина Ксения Михайловна, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), аспирант кафедры судебных экспертиз.

Адрес электронной почты: km.myskina@mail.ru

About the author:

Kseniya M. Myskina, Kutafin Moscow State Law University (MSAL), graduate student of Forensic Expertise's department.

E-mail: km.myskina@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКСПЕРТНЫХ УЧРЕЖДЕНИЙ В ЭПОХУ ЦИФРОВИЗАЦИИ

САРКИСЯН А.А.

Статья посвящена анализу информационной безопасности экспертных учреждений в условиях цифровизации. Рассмотрено современное состояние подготовки судебного эксперта в области защиты информации, выделены приоритетные направления модернизации профессии судебного эксперта в современных условиях. В результате проведенного исследования автор приходит к выводу о важности разработки политики информационной безопасности экспертных учреждений.

Ключевые слова: судебная экспертиза, судебный эксперт, специальные знания, цифровизация судебно-экспертной деятельности, цифровые следы, информационная безопасность, BYOD.

Цифровизация как процесс затрагивает различные направления развития судебно-экспертной деятельности, включая профессиональную подготовку судебных экспертов, развитие новых родов и видов судебных экспертиз, появление новых объектов и т.д. Однако в русле этой концепции практически не затрагивается вопрос информационной безопасности экспертных учреждений, что кажется удивительным, поскольку сложно отрицать влияния цифровизации на менеджмент СЭУ, на подходы к хранению и передаче данных, на развитие научно-технического оснащения СЭУ и на многие другие вопросы, которые имеют прямое отношение к самому процессу экспертного исследования.

Под информационной безопасностью судебно-экспертных учреждений нами понимается состояние информационной системы судебно-экспертного учреждения, при котором оно защищено от воздействия третьих лиц и разглашения конфиденциальной информации.

Для начала следует определиться, что именно будет являться объектами защиты. К ним следует отнести в первую очередь информационные ресурсы СЭУ, которые включают в себя всю документацию, имеющую отношение к деятельности СЭУ, лабораторий, к производству экспертиз и исследований, сведения о сотрудниках СЭУ. К объектам также относится любая конфиденциальная информация, ставшая известной сведущим лицам при производстве экспертиз и исследований, включая информацию, содержащую персональные данные.

К сожалению, нам уже кажется очевидным факт, что сотрудники различных организаций зачастую нарушают законодательство о персональных данных. Согласно ст.14 ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»¹ руководитель государственного экспертного учреждения обязан обеспечить условия, необходимые для сохранения конфиденциальности исследований и их результатов.

¹ Федеральный закон "О государственной судебно-экспертной деятельности в Российской Федерации" от 31.05.2001 г. N 73-ФЗ // Доступ из справ.-правовой системы «Консультант-Плюс».

Согласно ст.16 ФЗ о ГСЭД эксперт обязан не разглашать сведения, которые стали ему известны в связи с производством судебной экспертизы. Согласно ст.57 УПК, ст.85 ГПК, ст.49 КАС и ст.16 ФЗ о ГСЭД эксперт не вправе сообщать кому-либо о результатах судебной экспертизы, за исключением органа или лица, ее назначивших. За разглашение экспертом данных предварительного расследования предусмотрена уголовная ответственность по ст.310 УК. Однако административная ответственность, предусмотренная в случае разглашения данных, не касающихся вопросов предварительного расследования, может не оказать должного влияния на экспертов. Эксперты при производстве исследования имеют доступ к данным, которые могут стать объектами незаконной торговли информацией.

Интересным также кажется тот факт, что неразглашение информации специалистом наряду с судебным экспертом упоминается лишь в некоторых источниках, например, в ст.102 НК РФ указана ответственность сведущих лиц за разглашение налоговой тайны, в п.33.2 Приказа МВД №7 указана ответственность сотрудников ЭКП за разглашение информации, содержащей персональные данные¹, в ст.346 ТК ЕАЭС указано, что «специалист не должен разглашать, использовать в иных целях, передавать третьим лицам полученную им информацию, составляющую коммерческую, банковскую, налоговую или иную охраняемую законом тайну, а также иную конфиденциальную информацию, за исключением случаев, предусмотренных законодательством государств-членов²».

Заметим, что вопросы конфиденциальности данных тесно переплетены с этическим обликом сведущего лица. В кодексах экспертной этики «вопрос конфиденциальности информации рассматривается в рамках формулирования соответствующего принципа [1, с.130]». Эксперты должны трепетно относиться к информационной безопасности во избежание нанесения репутационного вреда всей системе судебно-экспертной деятельности. Утеря/утечка информации порождает недоверие общества ко всему институту.

Очевидно, что информационная безопасность СЭУ может быть нарушена третьими лицами. Несанкционированный доступ к информационным ресурсам, утечка и разглашение данных – реально существующий риск для организаций любого типа уже на протяжении многих лет. Судебно-экспертная деятельность тоже не является исключением. Например, в 2015 г. произошла серьезная утечка информации, включающей в себя также экспертные заключения ДЕА (Департамента по борьбе с наркотиками при Минюсте США) [4].

Одной из серьезных проблем для информационной безопасности является стратегия BYOD (bring your own device) [3], выраженная в использовании личных устройств в рабочем процессе. Зачастую сотрудникам проще использовать личное оборудование, которое может

¹ Приказ МВД России от 11.01.2009 № 7 «Об утверждении наставления по организации экспертно-криминалистической деятельности в системе МВД России» // [Электронный ресурс]: URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Centri/IEkspertno_kriminalisticheskij_centr/Osnovnie_normativno_prawovie_akti (дата обращения: 12.11.2020).]

² Таможенный кодекс Евразийского экономического союза (приложение N 1 к Договору о ТК ЕАЭС) // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_215315/ce19d6a6b4fdfa12a139639f9b2aca8438fd2141/ (дата обращения: 12.11.2020).

превосходить рабочие устройства по производительности, это ускоряет процесс и повышает работоспособность.

Сегодня это не видится особенной проблемой, однако если мы обсуждаем цифровизацию судебно-экспертной деятельности в качестве одного из средств перехода в цифровое пространство, то следует помнить о том, что использование устройств, защищенных только паролем, для хранения подобной информации, довольно опасно. Естественно, что мало кто использует хотя бы минимальные средства шифрования информации, тем более на личных устройствах.

Борьба со стратегией BYOD не должна выражаться бездумным запретом на использование личных устройств сотрудниками экспертных учреждений. Необходимо в первую очередь решить вопрос с компьютерно-техническим оснащением, предоставить в распоряжение экспертов устройства, с которыми им будет комфортно работать.

Стоит отметить, что важной составляющей информационной безопасности является доступность информации для авторизованных субъектов. В СЭУ доступ к информации предоставляется всем сотрудникам практически без ограничений. С точки зрения повышения эффективности и обучения сотрудников – это, несомненно, полезно. Однако, с другой стороны, вызывает вопрос, каковы же тогда пределы соблюдения конфиденциальности при производстве экспертиз и исследований.

Отдельно следует упомянуть, что цифровизация судебно-экспертной деятельности критикуется с позиции того, что она приведет нас к ‘Nintendo Forensics’ – ситуации, когда для проведения экспертного исследования будет достаточно нажатия одной кнопки. Маловероятно, что нас ждет подобная ситуация, поскольку использование достижений науки и техники лишь способствует ускорению процесса в части выполнения некоторых операций и обработки массива информации. Обработка конечных результатов и формирование вывода всегда будет являться прерогативой эксперта. Это связано в первую очередь тем, что системы подконтрольны тому, кто ими управляет [2, с.89-90].

Несомненно, что это довольно интересный вопрос для дискуссии, однако в этих размышлениях обычно не упоминается вопрос конфиденциальности данных, получаемых в результате работы автоматизированной системы. Не очень понятно, кем и каким образом будет осуществляться защита результатов исследований. Обслуживание подобных систем и оборудования требует специальных знаний, а перекладывать и эту обязанность на эксперта кажется излишним, поскольку это будет достаточно сильно влиять на загруженность эксперта.

Мы уже упоминали [2], что без фактического увеличения штата сотрудников использование современных технологий не будет давать ожидаемого результата, поскольку эксперты просто не будут успевать обрабатывать полученные данные. В данной ситуации, на экспертов ляжет еще обязанность по информационной защите данных. Кажется целесообразным введение роли специалиста по информационной безопасности в экспертных учреждениях, которому можно поручить большинство обозначенных задач.

Цифровизация судебно-экспертной деятельности порождает необходимость разработки политики безопасности СЭУ, в рамках которой будут определены основные

положения менеджмента СЭУ в области безопасности информации. В ближайшем будущем отсутствие профилактических мер в области информационной безопасности может стать серьезной проблемой для судебно-экспертных учреждений.

Библиографический список:

1. Мыскина К. М. Структура и содержание кодексов судебно-экспертной этики: сравнительный анализ // Вестник Университета имени О.Е. Кутафина. 2020. №6 (70). URL: <https://cyberleninka.ru/article/n/struktura-i-soderzhanie-kodeksov-sudebno-ekspertnoy-etiki-sravnitelnyy-analiz> (дата обращения: 29.10.2020).
2. Саркисян А.А. Профессия судебного эксперта в условиях цифровизации // Союз криминалистов и криминологов: периодическое печатное издание, журнал. — 2020. — № 1. С.87-93.
3. BYOD — удобство против безопасности // LukaSafonov от 13 апреля 2016, Habr // [Электронный ресурс]: URL: <https://habr.com/ru/post/281463/> (дата обращения: 12.11.2020).
4. DOJ Hacker Also Accessed Forensic Reports and State Department Emails // J.Cox от 12 февраля 2016 г., Motherboard tech by Vice // [Электронный ресурс]: URL <https://www.vice.com/en/article/qkjbwd/doj-hacker-also-accessed-forensic-reports-and-state-department-emails> (дата обращения: 29.10.2020).

References:

1. Miskina K.M. Structure and content of forensic expert ethics codes: comparative analysis // Courier of Kutafin Moscow State Law University (MSAL) 2020. №6 (70). URL: <https://cyberleninka.ru/article/n/struktura-i-soderzhanie-kodeksov-sudebno-ekspertnoy-etiki-sravnitelnyy-analiz> (date accessed: 29.10.2020). (In Russ.)
2. Sarkisian A. A. Forensic scientist in the digital era // The Union of Criminalists and Criminologists: periodical printed edition, bulletin. — 2020. — No. 1. P.87-93.
3. BYOD - convenience versus security // LukaSafonov, April 13, 2016, Habr (In Russ.)
4. DOJ Hacker Also Accessed Forensic Reports and State Department Emails // J.Cox, February, 12, 2016. (date accessed: 29.10.2020).

Anna Ash. Sarkisian

**INFORMATION SECURITY OF EXPERT INSTITUTIONS IN THE AGE OF
DIGITALIZATION**

The article is devoted to the analysis some features of the of information security of forensic institutions in the digital era, to consider the current state of the training of a forensic scientist in the field of information protection, to identify priority areas for the modernization of the profession of a forensic scientist in modern conditions.

As a result of the conducted research, the author concludes that the importance of the developing an information security policy for forensic institutions.

Keywords: Forensic science, forensic examination, forensic scientist, digital evidence, digitalization, information security, BYOD.

Сведения об авторе:

Саркисян Анна Ашотовна, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), аспирант кафедры судебных экспертиз.

Адрес электронной почты: annas.gp.117@yandex.ru

About the author:

Anna Ash. Sarkisian, Kutafin Moscow State Law University (MSAL), graduate student of Forensic Expertise's department.

E-mail: annas.gp.117@yandex.ru

ИСПОЛЬЗОВАНИЕ НЕТРАДИЦИОННЫХ ДЛЯ СУДЕБНО-ЭКСПЕРТНОЙ ПРАКТИКИ НАУЧНЫХ ДИСЦИПЛИН ДЛЯ ИССЛЕДОВАНИЯ МАТЕРИАЛОВ С ПОРНОГРАФИЧЕСКИМ ИЛИ ОСКОРБИТЕЛЬНЫМ КОНТЕНТОМ, РАЗМЕЩЕННЫХ В СЕТИ ИНТЕРНЕТ, КАК СПОСОБ ОБЪЕКТИВИЗАЦИИ РЕЗУЛЬТАТОВ ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

ТРОИЦКАЯ Т.А.

Сложившая экспертная практика уже перестает удовлетворять специфике, видовому и жанровому разнообразию размещенных в Сети Интернет материалов и во многом требует расширения своего аппарата не только путем назначения комплексных экспертиз, но и за счет обогащения самого понятийного и «операционного» аппарата с привлечением возможностей, методик и методов смежных либо обычно не затрагиваемых разделов тех же научных дисциплин. В статье на примере нескольких распространенных экспертных ситуаций предлагаются возможные алгоритмы разрешения сложившихся проблем путем повышения объективизации результатов экспертной деятельности за счет использования методов нетрадиционных для судебно-экспертной практики научных дисциплин гуманитарного и медицинского цикла (теории искусства, эстетики и философии, культурологии, сексологии). Предлагаемые варианты применения комплексного подхода должны предотвратить неоправданно узкий, предельно упрощенный и формальный подход эксперта или специалиста к разрешаемой проблеме. Обсуждаемые ситуации основаны на конкретных примерах из практики автора.

Ключевые слова: текст; визуальный объект; произведение изобразительного искусства; запрещенный контент; порнография; сексуальная риторика; культурология; эстетика.

В современной ситуации, когда цифровое пространство вошло практически в каждый российский дом [6, с. 274-298] и стало восприниматься пользователями одновременно и как часть их внутреннего мира, и как площадка для публичного самовыражения [3, с. 299-333], все более актуальными становятся не традиционные для моноэкспертиз (лингвистической, психологической, искусствоведческой, религиоведческой) вопросы. Ситуация усугубляется тем, что типичный пользователь сети Интернет одновременно ощущает себя и находящимся в интимном (приватном) пространстве, из чего проистекает убеждение, что «моя страница в социальной сети является только моей территорией», и в то же время использует неограниченные возможности данного вида коммуникации для запроса помощи, для выступления в роли учителя. Традиционно запрос о помощи от взрослых людей является частью практической деятельности психолога и психотерапевта, но в последние годы все популярней стало обращение с подобными запросами к анонимной аудитории в Интернете, который осуществляет своего рода атаку на живую коммуникацию [2, с. 157-159], для примерки на себя разных придуманных образов (наподобие аватаров), для выступления в разных социальных ролях и так далее.

В результате пользователи позволяют себе максимальную степень свободы проявления собственных желаний и эмоций при общении на публичных площадках, что выражается в публикации и скачивании материалов, связанных с различными проявлениями сексуальной жизни, потенциально оскорбительных, в том числе, не только для отдельного лица, но и для общественной морали и нравственности изображений, и т.п.

Причем, повышение вербальной агрессии, расширение спектра обсуждаемых тем в сторону традиционно табуированных наблюдается на внешне нейтральных ресурсах наподобие женских форумов (не подростковых) и дневниковых площадок. Публикуемые на них материалы имеют свою специфику и позволяют пользователям маскировать истинную тематическую и мотивационную направленность под нейтральными заголовками, так как модерация на подобных ресурсах основывается преимущественно на выборочном контроле заголовков и текста стар-топика. В результате на внешне безопасных ресурсах появляются многочисленные темы, в которых материалы о проблемах женского здоровья и физиологии практически со времени выхода темы, т.е. сразу же после опубликования, становятся формальным поводом для обсуждения преимуществ раннего начала половой жизни, инцеста, сопровождаются вульгарно-натуралистичными описаниями сексуального характера в советах и рекомендациях, якобы написанных от лица женщины (матери, которая якобы практикует подобный стиль воспитания в отношении своих родных детей, или же женщины, пережившей подобный опыт в детстве и юности). Или же обсуждение проблем, заявленных как планирование семейного бюджета, которые используются как повод для провокационных высказываний, тематически направленных против существующего государственного строя, политики, правительства РФ и главы государства, в частности.

В подобной ситуации сложившаяся экспертная практика уже перестает удовлетворять усложнившейся проблематике и во многом требует расширения не только за счет назначения комплексных экспертиз, но и за счет обогащения самого понятийного и «операционного» аппарата с привлечением возможностей, методик и методов смежных либо обычно не затрагиваемых разделов тех же научных дисциплин.

Обозначим несколько встретившихся нам на практике проблем:

Первая проблема: Использование в качестве защитной, оправдательной аргументации ссылок на то, что «спорный» креолизованный (визуальный или мультимедийный объект) является результатом творческой деятельности, а его создатель, будучи автором произведения современного актуального искусства, в принципе, вне зависимости от содержания выражаемого «контента» и его коммуникативной и мотивационной направленности не может быть подсуден, осуждаем.

Особенную актуальность этот аспект, широко представленный в заключениях специалистов, подготовленных по запросу стороны защиты, обретает в делах, касающихся изготовления и оборота порнографической продукции, пропаганды нетрадиционных сексуальных отношений и наркотических веществ несовершеннолетним лицам, а также в делах т.н. экстремистской направленности и в делах по оскорблению чувств верующих разных конфессий.

Хотя с точки зрения юриспруденции сам по себе факт относимости объекта к произведениям современного искусства, если только данный объект не отнесен к культурному наследию общенационального значения, не подразумевает автоматическое исключение его из числа потенциально «спорных» материалов, тем не менее подобные заключения, будучи опубликованными в СМИ, оказывают определенное негативное влияние на формирование общественного мнения и способствуют формированию потенциально конфликтных установок, особенно в среде творческой молодежи, внушая им мысль о «принципиальной неподсудности творца».

Представляется, что выход из данной ситуации может находиться не только в плоскости повышения правовой грамотности населения, но и в дополнении традиционного экспертного анализа, построенного, в основном, на методах судебной лингвистики и искусствоведения, методами эстетической оценки произведения искусства, основанными, вопреки расхожему мнению, не на вкусовщине, а на строгих научных критериях изучения восприятия и оценки художественного объекта личностью, зрителем, профессиональным зрителем и критикой.

Эстетика и теория искусства помогут ответить на вопрос о том, какие компоненты данного конкретного произведения направлены эстетическое восприятие потребителя [5, с. 87-145], в то время как психология восприятия и психология культуры помогут ответить на вопросы о механизме воздействия данного конкретного произведения на зрителя [1].

В существующей ситуации все сводится к безапелляционным суждениям одного или нескольких специалистов, как правило, имеющих научный или иной профессиональный интерес к исследуемому вопросу, о том, талантливо ли изображено представленное. Причем логика построения ответа в подобных «оправдывающих» заключениях всегда такова: данные произведения исполнены целиком от руки автором (поставлены, представлены на сцене под руководством автора и т.п.) – в них заложены творческие идеи, выражена душа, следовательно, любые формальные критерии оценки содержания и смысла в данном случае к результату творчества не применимы.

Представляется разумным, не оспаривая данный тезис, дополнить в экспертизе формально-содержательный анализ (что именно изображено) разрешением вопроса о том, как оно изображено и с какой целью (как повод для раскрытия совершенно иной темы, как способ шокировать зрителя и тем самым привлечь к себе внимание, как символ, который вызывает лишь отдаленные ассоциации со «спорным» объектом или предельно натуралистично как основная идея произведения), а также психологическим исследованием на тему восприятия и влияния на зрителя.

Поскольку современная наука не отрицает возможности любого произведения искусства и визуального объекта затрагивать не только когнитивную, но и эмоциональную сферу зрителя, и рассматривает процесс восприятия любого арт-объекта как психическую деятельность, то и исследовать данные объекты следует комплексно. Ведь каждый подобный объект, будучи введенным в публичное пространство, становится частью этого пространства и публичной коммуникации – следовательно, может быть оценен с точки зрения, что он сообщает публике, зрителю, обществу, как он подает изображенное, в привлекательном или отталкивающем ключе, какие эмоции и мысли формирует и т.п. Тем более, что даже

мировая история искусства знает случаи, когда знаменитым художником были созданы изображения, которые при всей их высоко художественности не были допущены для открытого публичного показа. Достаточно вспомнить, например, картину великого французского живописца Г. Курбе «Происхождение мира» 1866 года создания, которая более 120 лет не выставалась для широкого зрителя. Ведь для того, чтобы искусство было принято обществом одобрительно, оно должно, в том числе, соответствовать определенным социальным, культурным, политическим, психологическим и иным объективным условиям, определяемым в каждом конкретном случае индивидуально [4, с. 34].

Вторая проблема отчасти созвучна по своей природе рассмотренной выше и тоже связана с подменой понятий. Только если в предыдущем случае логика оправдания строится по принципу «если это продукт творческой деятельности, то он не может быть порнографией и т.п.», то в данном случае логика доказывания строится на половинчатости толкования сути запрета. Например, если в «спорных» изображениях с участием несовершеннолетних отсутствует демонстрация непосредственно половых органов, то это не порнографические материалы. В действительности же ст.242.1 УК РФ содержит прямые указания на то, какой именно материал с формально-содержательной, коммуникативной и мотивационной (объективной) точки зрения считается материалом с порнографическим изображением несовершеннолетних: должно в обязательном порядке включать в себя либо изображение полностью или частично обнаженных половых органов несовершеннолетнего, или изображение несовершеннолетнего лица, совершающего либо имитирующего иные действия сексуального характера.

То есть, исследуемые материалы должны содержать в себе изображение какого-либо проявления именно половой жизни несовершеннолетнего лица. К иным действиям сексуального характера, как и к проявлениям половой жизни, современные психология, сексология, сексопатология, научная, клиническая и экспертная практика относят в том числе так называемые аутоэротические действия, т.е. действия, которые напрямую связаны с проявлением половой жизни, с демонстрацией и представлением себя на снимке или видео именно как объекта вождения, с подчеркиванием своей роли только как полового партнера, с подчеркиванием признаков пола, направленных на то, чтобы вызвать (у определенной части зрителей) состояние полового возбуждения и разжечь нездоровый интерес к сексу с несовершеннолетними.

В число (перечень) таких действий, согласно общепринятой международной практике, входит и публичное демонстрирование лицом себя на камеру в обнаженном или полуобнаженном виде, с демонстрацией тех органов, которые традиционно в норме выступают как стимуляторы полового возбуждения и имеющие непосредственное отношение к половой жизни (в разных ее проявлениях). Сама по себе демонстрация, если она не обусловлена явными медицинскими, научными, иными приемлемыми с точки зрения общества, целями является проявлением и осуществлением действия сексуального характера – эксгибиционизм, и направлено на осуществление зрителем (реципиентом) другого действия сексуального характера (вуайеризм). Следовательно, для того, чтобы полностью и окончательно подтвердить или развеять сомнения относительно наличия или

отсутствия в представленном изобразительном контенте порнографии необходимо обязательное привлечение лица, сведущего именно в вопросах проявления жизни пола и секса, т.е. врача, реже – прошедшего специальную подготовку психолога, но одного заключения лингвиста или искусствоведа (киноведа, фотографа, режиссера) для ответа на данные вопросы будет явно недостаточно и формализованный подход тут, на наш взгляд, особенно недопустим.

Еще одна проблема связана с проблемой так называемой «сексуальной риторики».

С одной стороны, использование подобной лексики стало все более широким и прежние культуральные запреты для многих социальных групп и субкультур сегодня уже не действуют, с другой стороны, при возникновении какой-либо конфликтной и/или противоправной ситуации зачастую оценка подобных «текстов» получает сугубо формальное истолкование.

В частности, специалистом было обращено внимание на факт недооценки в экспертной практике культурных особенностей разных народов в отношении употребления так называемой «табуированной лексики».

На примере уличного жаргона можно видеть, что слова, вроде бы формально служащие только для обозначения половых органов и сексуальных действий используются для выражения широкого спектра эмоций, в том числе, для рассказа о событиях, совершенно не относящихся к любовно-эротической сфере. Причем, границы между уличным жаргоном, молодежным и профессиональным сленгом часто оказываются прозрачными.

Еще более актуальной данная проблематика становится, когда анализу подвергается речь представителей экспрессивных и эмоциональных «южных регионов» (Кавказ, Краснодарский край), особенно если представлены тексты, порожденные судебно-следственной ситуацией или же отбыванием наказания в местах лишения свободы.

Принято считать, что традиционная для нашей страны криминальная субкультура считала нежелательным использование обсценной (матерной) лексики – якобы в довоенное время считалось неприличным ругаться матом в камере и т.п. Однако расшифровки стенограмм аудиозаписей разговоров современных «криминальных элементов», в том числе, имеющих определенный вес и влияние в современной иерархии российского криминального мира, особенно в речи лиц из числа т.н. «воров» кавказского происхождения, демонстрируют высокую частотность и устойчивое использование подобной риторики в ситуации общения с лицами, равными им «по положению и статусу». При этом специфика ситуации не позволяет говорить о каком-либо любовно-эротическом или же прямом сексуальном подтексте.

Вообще, в речи людей, для которых русский язык не является родным, табуированная лексика и мат могут использоваться для достижения разных целей: это и презентация себя как свободно владеющего русским языком человека, и указания на собственную маскулинность и мачизм, часто обусловленные традициями регионального повседневного «негласного мужского этикета» щедро раздаваемые публичные обещания телесно унижить и надругаться в извращенной форме над своим обидчиком, не тождественные истинным намерениям коммуниканта.

В этом смысле вызывает определенное недоверие и буквальный подход к истолкованию устной экспрессивной речи между родственниками – так, представляется, что если в конфликтной ситуации муж, брат или отец обещает родственникам (детям, жене и т.д.) выступить в отношении них в качестве полового партнера, тем более насильника, истинность и буквальность его намерений должна быть специально доказана.

В этой ситуации представляется целесообразным привлечение к проведению экспертиз специалистов по межкультурной коммуникации, по бытовой культуре и даже специалистов по фольклору конкретного региона, местности, народа. Только с учетом анализа сложного комплекса факторов: взаимодействия традиционного и современного, городского и регионального, типичности отражения эмоций в устной речи того или иного народа, на основе анализа активного словаря, а также анализа представлений о допустимом и запретном, в том числе оскорбительном можно составить объективное и всестороннее аргументированное суждение по вопросу.

Подводя итог сказанному выше, следует отметить, что чем шире спектр привлекаемых смежных дисциплин, тем больше вероятность установления объективной истины в ходе экспертного исследования тех материалов, самостоятельное оценивание которых судебно-следственными органами невозможно.

Уход от моноэкспертиз призван не усложнить работу следователя и суда, а направлен на получение как можно более целостной картины произошедшего. Кроме того, он позволит в известной степени обезопасить традиционные виды гуманитарных экспертиз от непреднамеренных экспертных ошибок.

Библиографический список:

1. Анолли Луиджи. Психология культуры. Харьков: Издательство Гуманитарный Центр, 2016 480 с.
2. Гридаева Г.В. Атака на родительскую пару: всемогущество инцеста// Психиатрия и психоанализ: клинические диалоги. Материалы научно-практической конференции (25 марта 2017 года). М., 2017. С.157-159.
3. Иоскевич Я. Интернет как новая среда художественной культуры// Экранная культура. Теоретические проблемы. СПб.: «Дмитрий Буланин», 2012. С.299-333.
4. Кащенко Е.А. Sex: Реальный и виртуальный. М.: URSS, 2014. 192 с.
5. Салеев В.А. Искусство и его оценка. Минск, 1977. С.87-145.
6. Сергеева О. Компьютерный экран как элемент домашней повседневности//Экранная культура. Теоретические проблемы. СПб.: «Дмитрий Буланин», 2012. С.274-298.

References:

1. Anolli Luigi. Psychology of culture. Kharkov: Publishing House of the Humanitarian Center, 2016 480 p. (In Russ.)

2. Gridava G.V. The attack on the parental couple: the omnipotence of incest// Psychiatry and psychoanalysis: clinical dialogues. Materials of the scientific and practical conference (March 25, 2017). Moscow, 2017. Pp. 157-159 (In Russ.)
3. Ioskevich Ya. The Internet as a new medium of artistic culture// Screen culture. Theoretical problems. St. Petersburg: "Dmitry Bulanin", 2012. Pp. 299-333 (In Russ.)
4. Kashchenko E. A. Sex: Real and virtual. Moscow: URSS, 2014. 192 p. (In Russ.)
5. Saleev V. A. Art and its evaluation. Minsk, 1977. Pp. 87-145 (In Russ.)
6. Sergeeva O. Computer screen as an element of home everyday life // Screen culture. Theoretical problems. St. Petersburg: "Dmitry Bulanin", 2012. Pp. 274-298 (In Russ.)

Tatiana Al. Troitskaya

**THE USE OF NON-TRADITIONAL SCIENTIFIC DISCIPLINES FOR FORENSIC
EXPERT PRACTICE FOR THE STUDY OF MATERIALS WITH PORNOGRAPHIC OR
OFFENSIVE CONTENT POSTED ON THE INTERNET AS A WAY TO OBJECTIFY THE
RESULTS OF EXPERT ACTIVITY**

The established expert practice already ceases to meet the specifics, species and genre diversity of materials posted on the Internet and in many respects requires expanding its apparatus not only by assigning complex examinations, but also by enriching the conceptual and "operational" apparatus itself with the involvement of opportunities, techniques and methods of related or usually unaffected sections of the same scientific disciplines. In the article, on the example of several common expert situations, possible algorithms for solving the existing problems are proposed by increasing the objectification of the results of expert activity through the use of methods of non-traditional scientific disciplines of the Humanities and medical cycle (theory of art, aesthetics and philosophy, cultural studies, sexology). The proposed options for applying an integrated approach should prevent an unnecessarily narrow, extremely simplified and formal approach of an expert or specialist to the problem being solved. The situations discussed are based on specific examples from the author's practice.

Keywords: text; visual object; work of fine art; prohibited content; pornography; sexual rhetoric; cultural studies; aesthetics.

Сведения об авторе:

Троицкая Татьяна Александровна, Национальный общественный центр экспертиз, эксперт.

Адрес электронной почты: t.troizkaia@mail.ru

About the author:

Tatiana Al. Troitskaya, Association of experts to promote expertises "National Public Centre of expertise", expert.

E-mail: t.troizkaia@mail.ru

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КРИМИНАЛИСТИКИ И СУДЕБНОЙ ЭКСПЕРТИЗЫ

ВИДЫ ЭКСПЕРТИЗ, ПРОВОДИМЫХ ПРИ РАССЛЕДОВАНИИ ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

АБРАМОВА А.А., КУЧИН О.С.

Цель исследования – рассмотреть проблемные вопросы назначения, проведения экспертиз в процессе расследования финансирования терроризма. Кроме этого, в данной статье авторами анализируются некоторые ошибки следователей при взаимодействии с экспертными учреждениями. Вместе с тем, в данной статье раскрываются следующие виды экспертизы – лингвистическая, фонографическая, психологическая, религиоведческая, химическая, генетическая, взрывотехническая, баллистическая, трасологическая, психолого-психиатрическая, медицинская и другие. Авторы делают акцент на необходимости проведения компьютерно-технических экспертиз при расследовании финансирования терроризма. Такие экспертизы относятся к категории инженерно-технических экспертиз и проводятся по уголовным делам, где совершаются преступления с помощью компьютерной техники, других аппаратно-технических устройств и т.д. Так, в случае если финансирование терроризма совершалось с использованием электронных устройств, компьютеров, планшетов, телефонов и др., проведением компьютерно-технических экспертиз не следует пренебрегать. Следователь быстрее сможет установить истину по делу привлекая эксперта для поиска следов преступления на электронных устройствах. Выводы по результатам исследования заключаются в необходимости проведения по данной категории уголовных дел СКТЭ, производящих экспертные исследования в области IT-технологий.

Ключевые слова: финансирование терроризма, содействие терроризму, экспертиза, экспертное учреждение, эксперт, заключение эксперта, специальные знания, оперативно-розыскная деятельность, уголовное дело, расследование преступления, взаимодействие.

В уголовном судопроизводстве назначение, проведение экспертного исследования и последующее использование полученных заключений экспертов являются наиболее совершенной, основной и результативной формой использования специальных знаний.

Так, в процессе расследования преступления для проведения экспертиз привлекаются лица, обладающие специальными знаниями, определенной квалификацией, необходимой для формулирования определенных выводов в форме дачи заключения по вопросам, поставленным следователем в порядке уголовно-процессуального законодательства – эксперты (ст. 57 УПК РФ). Под специальными знаниями экспертов в законе понимаются профессиональные знания в науке, искусстве или ремесле, которыми не обладают другие участники уголовного судопроизводства. При этом из понятия

«специальные знания» исключаются профессиональные юридические знания, которыми оперируют в ходе расследования уголовного дела практические работники правоохранительных органов. [1, с.119]

В связи с этим в процессе расследования финансирования терроризма нередко возникает ситуация, при которой следователь, не обладая определенным объемом специальных знаний, в целях расследования преступления прибегает к знаниям эксперта. Такая необходимость их привлечения обуславливается тем, что преступниками: непрерывно разрабатываются различные схемы личной передачи, перечисления денежных средств на банковские счета, принадлежащие террористам и их соучастникам; создаются новые каналы финансирования; формируются иные методы финансовой помощи террористическим организациям.

Акцентируем внимание на то, что экспертиза назначается следователем как на стадии доследственной проверки, так и после возбуждения уголовного дела. При этом выбор эксперта, экспертной организации осуществляется по усмотрению органа, производящего следствие. Перед выбором эксперта следователю необходимо определить характер специальных знаний, которыми должен обладать субъект, а также вид экспертизы, затем определиться с экспертным учреждением, в котором будет производиться экспертиза. После этого необходимо вынести постановление о назначении судебной экспертизы и ознакомить с ними лицо с соответствующими материалами, в отношении которого было вынесено постановление, а также его адвоката. Алгоритм прост и ясен, однако не все следователи его выполняют должным образом.

Примером служит уголовное дело, рассмотренное Приволжским окружным военным судом. Так, в приговоре суд указал, что экспертизы по делу были проведены с нарушением прав подсудимых, поскольку в большинстве случаев заключения были даны экспертами, которые располагаются в ведомстве, возбудившем уголовное дело, что свидетельствует о наличии служебной зависимости и недостоверности их заключений¹.

Проведенный в ходе настоящего исследования анализ архивных данных показал, что в рамках расследования уголовных дел возбужденных по ч. 1.1 ст. 205.1 УК РФ, в большинстве случаев проводились экспертизы, указанные в таблице № 1.

Так, в 5 % случаев при расследовании финансирования терроризма следователи привлекали «специалистов в области языкознания» – экспертов-лингвистов. С их помощью были расшифрованы разговоры, установлено смысловое содержание текстов, выявлена завуалированная информация, содержащаяся в терминах и выражениях в устных разговорах террористов и письменных текстах. В связи с этим следует иметь ввиду, что при расследовании финансирования терроризма определение экспертами значения слова, произнесенного (написанного) террористом, его функции, направленности высказывания имеют доказательственное значение противоправности деяния.

¹ Уголовное дело № 1-2/2017 (1-13/2016) // Архив Приволжского окружного военного суда

Таблица № 1. Виды экспертиз проводимых в ходе расследования уголовных дел по ч. 1.1 ст. 205.1 УК РФ¹

№	Проведенные экспертизы	%
1	лингвистическая	5%
2	комплексная (лингвистическая, психологическая, психолого-религиоведческая)	15%
3	фонографическая	4%
4	судебно-химическая экспертиза наркотических средств	1%
5	химическая	0,5%
6	генетическая	0,5%
7	взрывотехническая	14%
8	баллистическая	14%
9	трасологическая	7%
10	психолого-психиатрическая	61%
11	судебная психическая экспертиза	39%
12	наркологическая	4%
13	судебно-медицинская	0,5%

В 15 % случаев при расследовании финансирования терроризма лингвистическая экспертиза проводилась в комплексе с другими видами экспертиз. Комплексной называется судебная экспертиза, в производстве которой участвуют эксперты двух и более специальностей (ст. 201 УПК РФ). Так, лингвистическая экспертиза в большинстве случаев проводилась в комплексе с психологической и психолого-религиоведческой. Психолого-лингвистическая экспертиза в основном назначается следователями, когда лицо отказывается от авторства (в содержании) исполненных им письменно или устно текстов. [2] Для ее качественного проведения эксперты должны иметь специальные знания в области психологии, психофизиологии, филологии, религиоведения. Задача экспертов заключается в установлении личных качеств автора и его психологического состояния в момент изложения текста. Кроме того, эксперт выявляет логику и идею изложения, содержание текста, степень участия и характер автора, его коммуникативные интенции, предмет, цель, реакции и др., то есть экспертом составляется речевой портрет человека.

Так, в одном из уголовных дел из заключения экспертов усматривалось, что в принадлежащем свидетелю Н. мобильном телефоне, изъятом при осмотре, содержалась переписка между ней и подозреваемым, в которой имелись психологические и лингвистические признаки побуждения, привлечения лица к участию в деятельности террористической организации «ИГИЛ» запрещенной организации на территории Российской Федерации, а также такие виды и приемы психологического воздействия, как

¹ Составлено авторами на основе анализа архивных уголовных дел Приволжского окружного военного суда; 2-ого Западного окружного военного суда; 1-ого Восточного окружного военного суда; Южного окружного военного суда за период с 2016-2019 г.

убеждение, внушение, манипуляция. Проведенная комплексная экспертиза позволила доказать, что эти виды воздействия использовались с целью побуждения и вовлечения свидетеля Н. к участию в деятельности указанной выше организации¹.

Следующий вид – психолого-религиоведческая лингвистическая экспертиза – несколько отличается от психолого-лингвистической тем, что дополнительно приглашается эксперт в области религиоведения с целью изучения идеологии текста, дачи заключения о наличии или отсутствии в содержании текста религиозного контекста, определения истинного вероучения исследуемой религиозной группы и т.д.

Так, в ходе проведенной по другому уголовному делу психолого-религиоведческой лингвистической экспертизы было установлено общее смысловое содержание предоставленных на исследование 15 видеофонограмм, зафиксированных на диске. Согласно заключению экспертов, смысл видеофонограмм был направлен на формирование в сознании адресата ненависти или вражды к людям, исповедующим другие религии, кроме радикального ислама. Кроме того, смысл был связан с пропагандой исключительности и превосходства мусульман, исповедующих фундаментализм (радикальное течение ислама), над мусульманами, исповедующими современный традиционный ислам. В видеофонограммах также содержались негативные установки в отношении вероотступников, неверных, неверующих (кяфиров), которые могли стать основой ненависти как чувств сильнейшей неприязни и враждебных настроений в отношении групп людей по признаку религиозной принадлежности и иных социальных групп (власти, спецслужб), а также мотивом к побуждению совершить насильственные действия против представителей различных иных религий, в том числе в отношении мусульман, относящихся к современным традиционалистам, а также к власти и спецслужбам.

Таким образом, экспертиза определила, что предоставленные материалы могут использоваться как единый комплекс средств пропагандистского психологического воздействия на сознание зрителей (адресатов), способный привести к возникновению в обществе ненависти или вражды по религиозному, национально-этническому и иному социальному признаку².

Кроме вышеперечисленных экспертиз, по данной категории дел назначалась в 4 % случаев фонографическая экспертиза. Она проводится в целях установления личности человека по голосовым, речевым признакам, которые находят отражение в фонограммах. Кроме того, фонограммы изучаются на предмет копирования, монтажа и других механических повреждений, специальных изменений. Также эксперты отвечают на вопросы, где и при каких обстоятельствах происходила беседа, то есть выясняют все технические подробности и другую информацию в отношении записи.

Терроризм, по своей природе, всегда представлял собой разновидность транснациональной организованной преступности. Террористические организации и террористы-одиночки успешно финансируют свою противоправную деятельность в ходе совершения других преступлений, таких как незаконный оборот оружия и его частей,

¹ Уголовное дело № 1-27/2018 // Архив 2-ого западного окружного военного суда

² Уголовное дело № 1-69/2017 // Архив 2-ого западного окружного военного суда

наркотических средств и психотропных веществ, захват заложников, совершение взрывов и поджогов и т.д. В связи с этим, специфика расследования преступлений террористического характера состоит в том, что в процессе раскрытия и расследования рассматриваемого вида преступления могут быть назначены самые различные виды экспертиз. Так, при расследовании финансирования терроризма и сопутствующих ему преступлений следователями проводились судебно-химическая экспертиза наркотических средств (1 %), химическая (0,5 %), генетическая (0,5 %), взрывотехническая (7 %), баллистическая (14 %), трасологическая (7 %).

Так, судебно-химическая экспертиза проводилась для изучения и дачи заключения о том, являются ли найденные в процессе следственных действий и оперативно-розыскных мероприятий вещества наркотическими средствами или психотропными веществами. Химическая экспертиза назначалась с целью изучения биологических и других жидкостей, позволяющего идентифицировать и определить качественный состав и характер вещества. Генетическая экспертиза проводилась с целью установления родства потерпевших после совершения террористического акта. Взрывотехническая экспертиза была назначена в целях исследования изделий, материалов, взрывчатых веществ, а также их остатков, которые были сохранены после совершенного взрыва. Баллистическая экспертиза проводилась для исследования найденного в процессе расследования преступления оружия и боеприпасов к нему в целях установления его индивидуальной идентификации и принадлежности. Трасологическая экспертиза помогла установить обстоятельства диагностического, идентификационного, ситуационного, классификационного характера оставленных на месте совершения преступления следов.

Из обязательных по данной категории дел проводились: экспертизы, определяющие психическое или физическое состояние подозреваемого, обвиняемого в целях определения субъективной стороны преступления – психолого-психиатрическая (61 %), судебная психическая экспертизы (59 %); психическое или физическое состояние подозреваемого, обвиняемого, в отношении которого имеются основания полагать, что он является больным наркоманией – наркологическая (4 %); судебные экспертизы в отношении потерпевших от лиц, осуществляющих террористическую деятельность, – судебно-медицинские (0,5 %).

Остается открытым вопрос о привлечении экспертов в сфере компьютерной информации при расследовании финансирования терроризма. Судебная компьютерно-техническая экспертиза (далее по тексту – СКТЭ), состоящая из аппаратно-компьютерной, программно-компьютерной, информационно-компьютерной, компьютерно-сетевой экспертизы, могла бы быть эффективно использована при расследовании финансирования терроризма. В ходе изучения уголовных дел нами было выявлено, что преступники часто финансируют терроризм при помощи компьютеров, планшетов, телефонов и других электронных устройств, но СКТЭ ни по одному факту не проводилась. Привлекались только специалисты и консультанты в области IT-технологий. На наш взгляд, один специалист в области информационных технологий не сможет заменить нескольких экспертов СКТЭ, в связи с чем рекомендуем приглашать специалистов только для помощи в осуществлении следственных действий, поиска, изъятия электронного устройства и передачи его в

экспертный отдел. Кроме того, специалист может оказать помощь в составлении перечня вопросов, которые будут поставлены перед экспертом. Проведенная СКТЭ по данной категории дел может дать следователю ответы на важные для расследования вопросы.

Первая группа ответов, полученных в рамках аппаратно-компьютерной экспертизы, даст информацию о технических характеристиках устройства, об исправности или неисправности технического устройства, об отклонениях от стандартных параметров устройства, об имеющихся на устройстве носителях информации, об исправностях накопителей памяти устройства и имеющейся на них информации и т.д.

Программно-компьютерная экспертиза позволяет дать информацию о представленном экспертам программном обеспечении и его компонентах, об имеющихся на устройстве программах, позволяющих переводить денежные средства дистанционно, о работоспособности программ, об имеющихся у программы функциях, о защитных функциях программ, о хронологии использования программ и т.д.

Третья, компьютерно-сетевая экспертиза, дает ответы об определении характеристик аппарата, об установлении места, роли, предназначения аппарата и подключении его к сети или серверу, об определении свойств вычислительной сети по ее отображению в информации носителей данных, о конкретных аппаратных устройствах, возможностях их применения для совершения финансирования терроризма и т.д.

Четвертая группа ответов дается в заключении информационно-компьютерной экспертизы. Она производится для получения информации о носителях цифровой компьютерной информации, об их форматировании, о виде записанных на них данных; о свойствах, состоянии и характеристиках носителя информации, о признаках защиты носителя информации; о данных, хранящихся на накопителе; о причинно-следственной связи между финансированием терроризма и действиями на электронном носителе и т.д.

Цифровая информация исследовалась многими учеными, такими как В.Б. Вехов, А.В. Геллер, Н.А. Зигура, Н.А. Сивидкая, П.Г. Смагин, М.В. Старичков, А.Ю. Чупрова и другими. Мы же представляем себе цифровую информацию как основу в организации и проведении СКТЭ. Под цифровой информацией мы понимаем зафиксированную на материальном носителе совокупность сведений, представленных в форме электрических сигналов, которые обращаются (обрабатываются, передаются, хранятся) в электронных устройствах, информационно-телекоммуникационной системе и сетях. В расследовании преступлений цифровая информация нередко становится виртуальными следами произошедшего преступления, так как имеет неразрывную связь с механизмом следообразования или некоторыми другими элементами криминалистической характеристики преступления (предметом и/или способом преступного посягательства).

Найденная на электронном устройстве и других носителях цифровая информация может быть нескольких видов – графическая (в виде схем, чертежей, фотографий и т.д.), звуковая (аудиозаписи, голосовые сообщения, голосовые команды и т.д.), текстовая (смс, чаты, переписка, заметки, календарные заметки и др.), числовая (коды, номера телефонов, пароли и т.д.), видеoinформация (видеозаписи, фильмы, ролики и т.д.). Кроме того, цифровая информация имеет идентификационный и диагностический вид. К

идентификационной (от латинского «identificare» – тождественность) цифровой информации относится информация, позволяющая установить существующее тождество с признаками общей родовой или групповой принадлежности. К примеру, копированные файлы, дубликаты, скриншоты, повторяющиеся запросы и т.д. К диагностической (от греческого «diagnosticos» – распознавание) цифровой информации относится информация, позволяющая выявить механизм события преступления, время происшествия, причинные связи, качественные и количественные характеристики объектов и их свойства и т.д. Примером диагностической может стать информация, позволяющая определить техническое состояние электронного устройства и других носителей цифровой информации, эксплуатацию, неполадки, объем и т.д.[5] Считаем, что, помимо вышеперечисленных видов, должен выделяться третий вид цифровой информации – комплексный, который одновременно включает в себя идентификационные и диагностические признаки, к примеру, информация, которая позволяет определить не только работоспособность программы, но и ее отношение к перечислению денежных средств террористам.

Таким образом, СКТЭ позволяет провести тщательное, всестороннее исследование аппаратного устройства, его программ, носителей информации и возможных подключений. Любая хранящаяся на электронном устройстве информация (приходящая по электронной почте, сфотографированная, записанная и т.д.), удаленная, зашифрованная или блокируемая охраняемыми программами, будет выявлена экспертами. Возможно, именно таким образом будут обнаружены иные акты, способы, источники финансирования терроризма.

Резюмируя вышеизложенное, отметим, что назначение и производство судебных экспертиз по данной категории уголовных дел являются основной процессуальной формой использования специальных знаний. Наиболее востребованными по делам о финансировании терроризма являются экспертизы в области медицины, психологии, психиатрии, религиоведения, теологии, фонографии, химии, баллистики, трасологии, а также IT-технологий. Помимо вышеперечисленных судебных экспертиз при расследовании финансирования терроризма могут быть проведены и иные виды экспертиз, связанных с финансированием терроризма. Очевидна неотвратимость внедрения проведения СКТЭ. Так, при расследовании финансирования терроризма рекомендуется помимо всех прочих экспертиз в обязательном порядке проводить СКТЭ, позволяющую не только изобличить лицо в его преступных действиях, но и обнаружить иные способы финансирования терроризма, что является значимым для дальнейших расследований. Во всех случаях проведения экспертиз не следует пренебрегать правилом о том, что их результаты напрямую зависят от выполнения следователем и экспертом всех законодательных требований, предъявляемых к их производству, а также от качества подготовки материалов, направляемых эксперту.

Библиографический список:

1. Баринов С.В. Кубанов В.В. Использование специальных знаний в расследовании преступных нарушений неприкосновенной частной жизни // Вестник Удмуртского

университета. Серия «Экономика и право». Вып. 1. Т. 25, 2015. с. 119 – 123.

2. Енгальчев В.Ф., Шипшин С.С. Судебно-психологическая экспертиза: методическое руководство [Электронный ресурс] URL: <http://yurpsy.com/files/ucheb/engal/011.htm> (дата обращения: 26.11.2020).

3. Себякин А.Г. Возможности использования контекстного поиска информации на компьютерных носителях в целях выявления, расследования и профилактики преступлений // Всероссийский криминологический журнал, 2019. № 2. Том 13. С. 262-270.

References:

1. Barinov S. V. Gubanov V. V. Use of special knowledge in the investigation of criminal violations of privacy // Bulletin of the Udmurt University. Series "Economics and law". Issue 1. Vol. 25, 2015. Pp. 119. 119-123. (In Rus)

2. Engalychev V. F., Shipshin S. S. Forensic psychological examination: methodological guide [Electronic resource] URL: <http://yurpsy.com/files/ucheb/engal/011.htm> (date accessed: 26.11.2020) (In Rus)

3. Sebyakin A. G. Possibilities of using contextual search for information on computer media in order to identify, investigate and prevent crimes / / all-Russian journal of criminology, 2019, no. 2. Volume 13. Pp. 262-270. (In Rus)

Oleg S. Kuchin, Alena Al. Abramova

TYPES OF EXPERTISE CONDUCTED IN THE INVESTIGATION OF TERRORIST FINANCING

The purpose of the study is to consider the problematic issues of appointment and conduct of expertise in the process of investigating the financing of terrorism. In addition, in this article, the authors analyze some mistakes made by investigators when interacting with expert institutions. At the same time, this article reveals the following types of expertise: linguistic, Phonographic, psychological, religious studies, chemical, genetic, explosive, ballistic, tracological, psychological and psychiatric, medical and others. The authors emphasize the need for computer-technical expertise in the investigation of terrorist financing. Such examinations belong to the category of engineering and technical examinations and are carried out in criminal cases where crimes are committed using computer equipment, other hardware and technical devices, etc.so, if the financing of terrorism was committed using electronic devices, computers, tablets, phones, etc., computer and technical examinations should not be neglected. The investigator will be able to establish the truth of the case faster by involving an expert to search for traces of the crime on electronic devices. Conclusions based on the results of the study are that it is necessary to conduct expert research in the field of IT technologies in this category of criminal cases.

Keywords: financing of terrorism, assistance to terrorism, expertise, expert institution, expert, expert opinion, special knowledge, operational search activity, criminal case, investigation of a crime, interaction.

Сведения об авторах:

Абрамова Алёна Алексеевна, Российский государственный университет правосудия, соискатель кафедры судебных экспертиз и криминалистики.

Адрес электронной почты: alena-abramova-90@bk.ru

Кучин Олег Стасьевич, Российский государственный университет правосудия, профессор кафедры судебных экспертиз и криминалистики, доктор юридических наук, доцент, Академик РАЕ, Заслуженный деятель науки и техники РАЕ.

Адрес электронной почты: kuchin-os@rambler.ru

About the authors:

Alena Al. Abramova, Russian State University of Justice, Department of forensic examinations and criminalistics, candidates for a degree of candidate of science.

E-mail address: alena-abramova-90@bk.ru

Oleg S. Kuchin, Russian State University of Justice, Professor of the Department of forensic examinations and criminalistics, Doctor of Sciences (Law), Professor, Academician of RAS, Honored worker of science and technology.

E-mail address: kuchin-os@rambler.ru

ГРИГОРОВИЧ В.Л.

Рассматриваются дискуссионные вопросы о понятии и предмете криминалистической одорологии. На основе анализа предмета и обобщения существующих дефиниций предлагается целесообразным включить в предмет криминалистической одорологии ряд научно обоснованных закономерности, изложенных в статье, а также авторское определение криминалистической одорологии.

Ключевые слова: криминалистическая одорология, биодетектор, ольфактроника, одорологическое исследование, следы запаха, запаховая информация, научно-технические средства, одорологическая экспертиза.

На сегодняшний день представление о криминалистической одорологии непосредственно связано с проблемами развития этой научной отрасли. Современное развитие теории криминалистической одорологии несколько приостановилось в связи с рядом причин, с одной стороны, это вызвано отсутствием согласованности между учеными (криминалистами, процессуалистами и биологами) и креативных научных исследований в этой области, с другой – настойчивым навязыванием некоторыми биологами укрепившейся на практике экспертной формы проведения исследований следов пахнущего вещества, выделяемого человеком¹, с использованием служебно-розыскных собак (биодетекторов) как единственно возможной [13, с. 46–52]. Указанные обстоятельства обусловили возникновение следующих аспектов проблемы развития криминалистической одорологии: во-первых, экспертами-биологами, занимающимися исследованиями следов пахнущего вещества, выделяемого человеком, предпринимается попытка подменить формирующуюся научную теорию криминалистической одорологии ольфактроникой [12], от которой отказались еще в шестидесятые годы прошлого века, отдав предпочтение одорологии. Во-вторых, наблюдается спад интереса научной общественности к определению предмета криминалистической одорологии и полемике о процессуальной форме закрепления результатов исследования следов пахнущего вещества вследствие внедрения в криминалистическую практику одорологической экспертизы. В-третьих, еще не сформировалось однозначное отношение к функциональным способностям биодетекторов. В-четвертых, имеет место гипертрофирование экспертами-одорологами роли биодетекторов в «идентификации»² источников запаха по их следам.

¹ В данном случае под следами пахнущего вещества человека нами понимаются следы свободных жирных кислот липидной фракции плазмы крови, которые выделяются с потовым секретом и обладают определенной летучестью и индивидуальностью для каждого человека.

² В таком контексте использование этого термина является спорным, так как узнавание биодетектором источника запаха напоминает идентификацию по мысленному образу, которая в теории и практике криминалистики и уголовного процесса применяется в форме следственного опознания, осуществляемого человеком, кроме того, имеются сомнения в

Безусловно, все упомянутые аспекты рассматриваемой проблемы существенно препятствуют развитию теории криминалистической одорологии, в формирование которой внесли определенный вклад работы В.Д. Басая, П.Д. Биленчука, А.И. Винберга, О.Г. Гвахария, О.А. Грошениковой, А.А. Кириченко, М.В. Салтевского, В.И. Старовойтова, К.Т. Сулимова, А.А. Топоркова, Г.В. Фёдорова и других ученых. Указанные аспекты можно подразделить на искусственно созданные или надуманные (попытка подменить одорологию ольфактроникой, внести сомнения в функциональные способности биодетекторов и, наоборот, гипертрофировать их роль в исследовании следов пахнущего вещества) и фундаментальные, то есть принципиально влияющие на формирование теории криминалистической одорологии (например, определение процессуальной формы закрепления результатов одорологического исследования). Все эти аспекты взаимосвязаны и существенно влияют на постановку акцента в умозаключениях в зависимости от логической посылки. Так, утверждение о необходимости создания ольфактроники как самостоятельного направления в криминалистической экспертизе основывается на мнении о незаменимости биодетекторов в распознавании индивидуального запаха человека и необходимости проведения биоанализа следов пахнущего вещества в форме экспертизы.

Термин «ольфактроника» (от лат. *olfactus*) означает запах для обозначения науки об обонянии и соотносится с одорологией как частное к общему. О том, что одорологическое исследование по своему содержанию шире исследования, проводимого с использованием биодетектора, отмечал в свое время В.А. Снетков. «Так как в принципе выборка по запаху – писал он – возможна с использованием технических и иных средств (например, газоанализаторов), наиболее точным представляется термин «кинологическая идентификация» или, с учетом устоявшейся терминологии – «кинологическая выборка» в отличие от часто использующего в этом смысле термина «одорологическая (запаховая) идентификация» как более широкого по смыслу» [11, с. 12].

Исследование понятия криминалистической одорологии показывает, что существуют различные подходы к ее определению. Под криминалистической одорологией понимают учение о запахах с целью установления личности [15, с. 331] или запахоносителей, их вещей, предметов, следов и иных объектов с помощью обоняния специально для этого отдрессированных служебно-розыскных собак, а также изучение механизма распознавания запахов [3, с. 52–57]; одно из направлений криминалистики, суть которого состоит в извлечении, сохранении и использовании запаховой информации в целях раскрытия и расследования преступлений [10, с. 3]. Несколько пространную формулировку судебной одорологии предлагает А.А. Кириченко, который трактует ее как «раздел криминалистики, разрабатывающий на основе познания закономерностей возникновения, функционирования, исчезновения, собирания, внеэкспертного и экспертного исследования следов запаха, оценки и использования запаховой информации, которая добыта от любых объектов при помощи обоняния собаки, гласные технические средства, тактические приемы и методические рекомендации по предупреждению, выявлению, пресечению, раскрытию,

существовании совокупности индивидуальных признаков на генетическом уровне, приводящих к 100 % совпадению запаховых проб.

предварительному расследованию преступлений, а также судебному разрешению уголовных дел и исполнению судебных решений» [8, с.58]. А.А. Топорков рассматривает криминалистическую одорологию как отрасль криминалистической техники, которая представляет собой систему научных приемов и технических средств обнаружения, анализа, изъятия и хранения запаховых следов для их последующего использования на предварительном следствии в целях установления конкретного человека и принадлежащих ему предметов, вещей, документов и иных объектов по индивидуальному запаху [7, с. 204]. Другие определения криминалистической одорологии, по своей сути, близки к приведенным и отличаются друг от друга лишь некоторыми характеризующими признаками (например, отнесением ее к направлению либо разделу криминалистики или отрасли криминалистической техники) [14, с. 16–19].

Во всех определениях криминалистической одорологии либо прямо указывается, либо подразумевается использование обонятельных способностей биологических анализаторов запаха (например, служебно-розыскной собаки), а также предлагается изучение механизма распознавания запахов. Отсюда следует, что криминалистическая одорология полностью включает в себя ту часть ольфактроники, которая используется в криминалистических целях (криминалистическую ольфактроникку) и нет необходимости выделять ее в самостоятельное научное направление либо отрасль.

Вместе с тем во многих определениях криминалистической одорологии ограничен ее предмет и превалирует та часть, которая призвана изучать обонятельные способности животных для их использования в распознавании источников запаха по оставляемым ими следам пахнущего вещества. Это, видимо, и послужило мотивом, побудившим некоторых экспертов-биологов предпринять попытку подменить криминалистическую одорологию ольфактроникой.

Изучение предмета криминалистической одорологии убеждает в необходимости включить в ее структуру ту часть ольфактроники, которая обозначала бы исследование пахнущих следов человека с помощью биодетекторов и определить ее, например, как ольфакторный «биоанализ» (в данном случае этот термин использован в связи с тем, что некоторые ученые определяют ольфактроникку как инструментальную одорологию [10, с. 204–205]), при этом доминирование его над другими структурными элементами криминалистической одорологии недопустимо.

Указанные выше обстоятельства обуславливают также необходимость уточнения предмета криминалистической одорологии. Основываясь на методологическом приеме исследования – от общего к частному, предмет криминалистической одорологии следует определять через предмет одорологии как более общей научной отрасли. Первые попытки определения предмета одорологии предприняты М.В. Салтевским, который отмечал: «Предметом одорологии является запах, его природа, закономерности образования, механизм обнаружения и восприятия запаха, а, следовательно, раскрытие психофизиологической природы обоняния» [10, с. 5].

Ряд ученых подразделяют предмет криминалистической одорологии на такие группы закономерностей, как: а) образование, функционирование, исчезновение запаха и

связанных с ним явлений [1, 2]; б) физические и биологические закономерности образования следов запаха [9, с. 279]; в) механизм образования запаховых следов [5, с. 5]; г) возникновение, функционирование, исчезновение, собирание, внеэкспертное и экспертное исследование следов запаха; д) оценка и использование запаховой информации [8, с. 58].

В первой группе закономерностей, предлагаемой П.Д. Биленчуком, Н.С. Золотарем, Е.Г. Коваленком и А.А. Марчуком, не совсем понятно о каких именно связанных с запахом явлениях идет речь, также спорной является формулировка четвертой группы закономерностей, очерченной А.А. Кириченко, в части функционирования, экспертного и внеэкспертного исследования следов запаха.

В этой связи представляется целесообразным включить в предмет криминалистической одорологии следующие закономерности:

1. Процесс формирования запаха и механизм образования следов пахнущего вещества. Последние являются производными от запаха и поэтому состоят с ним в причинно-следственной связи. Представляя собой часть целостного явления, механизм образования следов пахнущего вещества невозможно объяснить, не рассмотрев процесс формирования запаха.

2. Механизм восприятия запаха и распознавания источников их продуцирования биодетекторами (обоняние). Восприятие запаха представляет собой «ощущение, которое возникает у человека и животных в результате действия определенных химических веществ на обонятельные рецепторы» [6, с. 25].

3. Процессы собирания, сохранения и исследования следов пахнущего вещества. Это три вида целенаправленной совместной деятельности органов уголовного преследования и специалистов в области криминалистической одорологии, которая обращена на получение фактических данных, используемых для установления обстоятельств, подлежащих доказыванию по уголовному делу.

4. Механизм использования разработанных на основе научных положений технических средств, тактических приемов и рекомендаций собирания, сохранения и исследования следов пахнущего вещества, а также полученных в результате этого фактических данных в целях предупреждения, раскрытия и расследования преступлений [4, с. 54–55].

На основе анализа предмета и обобщения существующих дефиниций мы пришли к выводу что под криминалистической одорологией следует понимать отрасль криминалистической техники, представляющую собой систему научных положений, раскрывающих закономерности процесса формирования запаха, механизма образования следов пахнущего вещества, его восприятия и распознавания, а также разработанных на их основе технических средств тактических приемов и рекомендаций собирания, сохранения, исследования и использования запаховой информации в целях предупреждения, выявления и расследования преступлений.

Библиографический список:

1. Биленчук П.Д. Методические аспекты одорологии (науки о запахах) / П.Д. Биленчук, А.А. Марчук // Теоретические и практические проблемы обеспечения раскрытия и расследования преступлений криминалистическими методами: сб. ст. / Украин. Акад. внутрен. дел. Киев, 1992. С. 26–27.
2. Биленчук П.Д. Криминалистическая одорология в раскрытии и расследовании преступлений: метод. пособие / П.Д. Биленчук, Н.С. Золотарь, Е.Г. Коваленко. Киев: РИО МВД Украины, 1994.
3. Винберг А. И. Криминалистическая одорология / А.И. Винберг // Социалист. законность. 1971. № 11. С. 52-57.
4. Григорович В. Л., Фёдоров Г. В. Инновационные направления развития криминалистики: монография / под ред. Г.В. Фёдорова. М.: Юрлитинформ, 2012. 272 с.
5. Грошенкова О. А. Исследование запаховых следов человека при расследовании преступлений: учеб.-метод. пособие / О.А. Грошенкова. Саратов: СГАП, 1999.
6. Использование консервированного запаха в раскрытии преступлений: учеб. пособие / М.В. Кисин [и др.]; под ред. М.В. Кисина. М., Берлин: ВНИИ МВД СССР; КИННП МВД ГДР, 1983.
7. Ищенко Е. П. Криминалистика: учебник / Е.П. Ищенко, А.А. Топорков; под ред. Е.П. Ищенко. М.: Юрид. фирма «КОНТАКТ»; ИНФРА-М, 2003. 748 с.
8. Кириченко А. А. Проблемы судебной одорологии: монография / А.А. Кириченко. Харьков: Основа, 1997.
9. Салтевский М. В. Криминалистика: учеб.-практ. пособие / М.В. Салтевский. Харьков: Рубикон, 1997.
10. Салтевский М. В. Криминалистическая одорология: лекция для студентов фак. повышения квалификации / М.В. Салтевский. Киев: Киев. высш. шк. МВД СССР, 1976.
11. Снетков В. А. Кинологическая выборка / В.А. Снетков // Использование консервированного запаха в раскрытии краж и преступлений против личности : материалы Всесоюз. семинара-совещания; МВД Латвийской ССР, Всесоюз. науч.-исслед. ин-т МВД СССР. Рига, 1984.
12. Старовойтов В. И. Запах и ольфакторные следы человека / В.И. Старовойтов, Т.Н. Шаманова. М. : ЛексЭст, 2003. 128 с.
13. Старовойтов В. И. Судебная экспертиза – единственно допустимая процессуальная форма ольфакторного исследования пахнущих следов человека / В.И. Старовойтов // Вестн. криминалистики. 2003. Вып. 2 (6). С. 46-52.
14. Фёдоров Г. В. Одорология: запаховые следы в криминалистике / Г.В. Фёдоров. Минск: Амалфея, 2000. 144 с.
15. Энциклопедия судебной экспертизы / Т.В. Аверьянова [и др.] ; под ред.: Т.В. Аверьяновой, Е.Р. Россинской. М.: Юристъ, 1999.

References:

1. Bilenchuk P.D. Methodological aspects of odorology (science of odors) / P.D. Bilenchuk, A.A. Marchuk // Theoretical and practical problems of ensuring the disclosure and investigation of crimes by criminalistic methods: collection of articles. Art. / Ukraine. Acad. internal cases. Kiev, 1992. P. 26–27. (In Russ.)
2. Bilenchuk P.D. Forensic odorology in the disclosure and investigation of crimes: method. manual / P.D. Bilenchuk, N.S. Zolotar, E.G. Kovalenko. Kiev: Ministry of Internal Affairs of Ukraine, 1994. (In Russ.)
3. Vinberg A.I. Forensic odorology / AI Vinberg // Socialist. legality. 1971. №. 11. P.52-57. (In Russ.)
4. Grigorovich V.L., Fedorov G.V. Innovative directions of development of criminalistics: monograph / ed. G.V. Fedorov. Moscow: Yurlitinform, 2012. 272 p. (In Russ.)
5. Groshenkova O.A. Research of human odor traces in the investigation of crimes: study guide. allowance / OA Groshenkov. Saratov: SGAP, 1999. (In Russ.)
6. Use of canned smell in crime detection: textbook allowance / MV Kissin [et al.]; ed. MV Kissin. Moscow, Berlin: All-Russian Research Institute of the Ministry of Internal Affairs of the USSR; KINNP Ministry of Internal Affairs of the GDR, 1983. (In Russ.)
7. Ishchenko E.P. Forensic science: textbook / E.P. Ishchenko, A.A. Toporkov; ed. E.P. Ishchenko. M.: Jurid. firm "CONTACT"; INFRA-M, 2003. (In Russ.)
8. Kirichenko AA Problems of forensic odorology: monograph / AA Kirichenko. Kharkov: Osnova, 1997. (In Russ.)
9. Saltevsy M.V. Criminalistics: training manual/ M.V. Saltevsy. Kharkiv: Rubicon, 1997. (In Russ.)
10. Saltevsy M.V. Forensic odorology: lecture for students of faculty. advanced training / M.V. Saltevsy. Kiev: Kiev. higher. shk. Ministry of Internal Affairs of the USSR, 1976. (In Russ.)
11. Snetkov V.A. Cynological sampling / VA Snetkov // The use of canned smell in the disclosure of thefts and crimes against the person: materials of the All-Union. seminar-meeting; Ministry of Internal Affairs of the Latvian SSR, All-Union. scientific research Institute of the Ministry of Internal Affairs of the USSR. Riga, 1984. (In Russ.)
12. Starovoitov V.I. Forensic examination is the only admissible procedural form of olfactory research of smelling human traces. Starovoitov // Vestn. forensics. 2003. Issue. 2 (6). P.46-52.
13. Starovoitov V.I. Smell and olfactory traces of a person / V.I. Starovoitov, T.N. Shamonova. M.: LeksEst, 2003. 128 p. (In Russ.)
14. Fedorov G.V. Odorology: odor traces in criminalistics / G.V. Fedorov. Minsk: Amalfeya, 2000. 144 p. (In Russ.)
15. Encyclopedia of forensic examination / T.V. Averyanov [and others]; ed.: T.V. Averyanova, E.R. Rossinskaya. M.: Yurist, 1999. (In Russ.)

Vasily L. Grigorovich

ON THE CONCEPT AND SUBJECT OF CRIMINALISTIC DOROLOGY

The article deals with debatable questions about the concept and subject of judicial odorology. Based on the analysis of the subject and generalization of existing definitions, it is proposed to include in the subject of judicial odorology a number of scientifically based regularities set out in the article, as well as the author's definition of judicial odorology.

Keywords: forensic odorology, biodetector, olfactronics, odorological research, odor traces, odor information, scientific and technical means, odorological examination.

Сведения об авторе:

Григорович Василий Леонидович, Белорусский государственный университет, юридический факультет, доцент кафедры криминалистики, кандидат юридических наук, доцент,

Адрес электронной почты: gylmail@mail.ru

About the author:

Vasily L. Grigorovich, Belarusian State University, Law Faculty, Associate Professor of the Department of Criminalistics, Candidate of Sciences Law, Docent.

E-mail: gylmail@mail.ru

ПРОБЛЕМЫ ОДОРОЛОГИЧЕСКОЙ ДЕТЕКЦИИ ЗАПАХОВЫХ СЛЕДОВ КАННАБИСА: ОПЫТ США

ХОЛЕВЧУК А.Г, УВАРОВ А.В.

В практической деятельности правоохранительных органов США одорологическая детекция каннабиса может служить основанием проведения необоснованных процессуальных действий (обысков автомобилей) в разных юрисдикциях США. Источником запаха в таких случаях часто является высушенный цветок конопли, содержащийся в различных упаковочных материалах. В исследовании рассмотрен вопрос о том, как влияет вид упаковки на выявление запаха каннабиса. Проведена оценка двух видов каннабиса и пяти типов упаковки. Неподготовленные участники исследования были ознакомлены с контейнерами, после чего им было предложено, исходя из запаховых ощущений выбрать в каком контейнере находятся образцы каннабиса, в другом контейнере с идентичными характеристиками отсутствовали образцы. Результаты показывают, что открытый и случайно упакованный каннабис детектируется с высокой степенью точности, тогда как материал, упакованный в двойной герметичный пластиковый пакет, идентифицируется случайным образом. Полученные результаты могут способствовать решению проблем, связанных с обнаружением каннабиса по запаховым следам правоохранительными органами, и в других случаях.

Ключевые слова: каннабис; обнаружение запаха; обонятельная способность; запах; обнаружение наркотиков.

Введение.

В североамериканской криминалистике обращается внимание на то, что сухие цветки полевой конопли (*Cannabis sativa L.*) имеют характерный и легко определяемый запах. Данный вывод делается исходя из анализа множества рапортов полиции и судебных решений, он служит основой для формирования доктрины «очевидного запаха», касающейся порядка выдачи компетентными органами ордеров для проведения обысков [1,2,3]. Тем не менее, эмпирическая основа для таких утверждений не имеет достаточного научного обоснования. В частности, несмотря на то, что летучие соединения в цветке каннабиса тщательно изучены с помощью аналитической химии, до недавнего времени отсутствовало систематизированное, эмпирическое описание его аромата.

Современные исследования с помощью количественной сенсорной оценки показывают, что запах конопли не является однородным: отдельные штаммы (сорта) имеют отличительные запаховые характеристики. В практической деятельности правоохранительных органов США в соответствии с положениями доктрины «очевидного запаха», допускается беспрепятственный обыск транспортного средства в случае выявления офицером полиции запаха каннабиса, даже в случае, если он скрыт и распространяется из

сумки или другого места. Эмпирические данные о запаховой детекции конопли незначительны. Одно из доступных исследований, в котором описываются обстоятельства трех случаев задержания в штате Нью-Джерси США, показывает, что требования, выдвинутые сотрудниками полиции перед проведением обыска, были не обоснованы [6]. В решении суда [7] также ставятся вопросы о запаховом восприятии каннабиса в связи с заявлениями полиции.

В анализируемом исследовании [19] оценена возможность проведения запаховой детекции сухих цветков каннабиса, упакованных случайным образом, как правило, встречаемого при остановке транспортных средств, а также в более сложном типе упаковки, а именно, в вакуумной пластиковой упаковке. Исследователи выполняют эксперимент с помощью относительно простой техники сдерживания свободного пространства и сенсорной методологии принудительного выбора с двумя альтернативами.

2. Материалы и методы.

Этический аспект.

Протокол исследования одобрен Институциональным советом по социальной, поведенческой и образовательной деятельности Государственного университета Колорадо (США), протокол № 18-8050H. Каждый участник предоставил письменное согласие. Все участники ни разу не вступали в непосредственный контакт с образцами каннабиса. Розничная продажа данного наркотического средства для совершеннолетних возрастной группы от 21 года и старше разрешена в штате Колорадо США с 1 января 2014 года.

2.2. Участники.

Участники эксперимента подбирались путем размещения бюллетеня на доске объявлений местного сообщества. Текст гласил, что приглашаются к участию в исследовании лица, употребляющие, не употребляющие или употреблявшие каннабис. Участники отбирались с учетом возрастных характеристик (от 21 до 50 лет). За участие в исследовании участникам было выплачено по 20 долларов США.

2.3. Образцы каннабиса.

Образцы каннабиса были приобретены в двух аптеках города Форт-Коллинс США, лицензированных на розничную торговлю в штате Колорадо: районные аптеки Ливуэлл и Вертс. Приобретены по одной унции (28 граммов) высушенных цветков конопли Golden Goat и Mob Boss. Данные сорта выбраны для представления ароматической вариативности, имеющейся у разных сортов каннабиса. Предыдущая количественная сенсорная оценка [4,5] показывает, что данные сорта имеют различные запаховые профили, например, аромат, исходящий от Golden Goat описывается как цитрусовый, сладкий, острый; Mob Boss – грубоватый, древесный и травяной.

Наименования образцов, предоставленных аптеками, используется для удобства. Их применение не подразумевает позицию относительно таксономической действительности или ботанического происхождения любого образца.

2.3. Упаковка исследуемых образцов каннабиса.

Каждый образец каннабиса был разделен на 5 пятиграммовых частей для использования в испытаниях по одорологической детекции, а также одна часть массой 3 грамма использовалась для предварительного ознакомления с запахом (см. п. 2.4).

Образцы каннабиса были представлены в пяти разных вариациях:

- 1) в открытой стеклянной чашке объемом 6 унций (177 мл.);
- 2) внутри закрывающегося полиэтиленового пакета для еды зип-типа размером 17,7 x 18,8 см (Ziploc® Quart Storage Bags, S. C. Johnson & Son, Inc.);
- 3) внутри плотного полиэтиленового пакета размером 38x50 см (Crown Poly Pull-N-Pak®);
- 4) внутри сертифицированного детского полипропиленового контейнера поп-топ (XIT® Brand Products) объемом 30 драм (110,9 мл);
- 5) внутри двойного вакуумного контейнера для хранения пищевых продуктов (Mainstays™ Vacuum Sealer Rolls,) размером 11 дюймов на 16 футов (28 x 487,7 см), сделанный из полиэтилена и нейлона, закрытый с помощью Ziploc® V203 Vacuum Sealer Machine.

Каждый образец каннабиса совмещался с контрольным образцом, состоящим из идентичной, но пустой упаковки. Образцы каннабиса и контрольные образцы хранились в стеклянных банках в морозильной камере при -2 °C и перед тестированием размораживались при комнатной температуре в течение 2 часов.

2.3. Камеры отбора образцов запаха.

Каннабис и пустые образцы были размещены в камере отбора образцов запаха, что позволило участникам тестирования детектировать летучие вещества. Камеры представляли собой 2 американских галлона (7,6 л) белых HDPE-ведер (Leaktite, Leominster, MA) со снятыми ручками и накрытыми двумя белыми крышками того же производителя. Прямоугольное отверстие размером 7x7 см (касающееся внутренней окружности приподнятого края крышки) было разрезано на одну крышку, чтобы обеспечить обнаружение запаха. Затем неперфорированная крышка помещалась поверх крышки с портом, что позволило пробам запаха аккумулироваться во внутреннем свободном пространстве ведра. Неперфорированная верхняя крышка удалялась непосредственно перед анализом запаха участником и заменялась сразу после. Буквенно-цифровой код (помещенный на ведро и крышку напротив стороны, обращенной к участнику теста) однозначно идентифицировал каждый образец для администратора теста и давал сигнал выравнивания для порта анализатора. Каннабис и контрольные образцы установлены в камеры отбора образцов запаха за один час до тестирования. Тент из сложенной алюминиевой фольги размещался свободно над каждым раздражителем/пустышкой в целях обеспечения дополнительного визуального контроля, способствуя свободной циркуляции воздуха вокруг раздражителя/пустышки.

2.4. Процедура тестирования.

Участник садился за стол и надевал маску для сна (Mack's® Dreamweaver™ Contoured Sleep Mask). Две камеры для отбора проб запаха размещались перед ним. Задача состояла в том, чтобы, используя обоняние, проанализировать каждую камеру и указать ту, в которой

содержится каннабис. Десять пар образцов (образец каннабиса и соответствующий образец пустой упаковки) показан в случайном порядке каждому участнику. Кроме того, размещение проб и образцов каннабиса слева-направо было рандомизировано по всем испытаниям для каждого участника.

Участникам разрешалось исследовать камеры отбора проб запаха столько раз, сколько необходимо для принятия решения. Перед испытанием участнику показывали пустую камеру для отбора проб и разрешали попрактиковаться понюхав ее. Также участник нюхал 5 грамма образца Golden Goat и Mob Boss из одной банки объемом 1 американская пинта (473 мл), чтобы ознакомиться с запахом.

3. Результаты.

3.1. Демографические характеристики участников.

В тестировании участвовал 21 человек (11 мужчин и 10 женщин) возрастом 21 год и старше (в среднем $29,7 \pm 7,6$ лет). Все участники сообщили, что приобрели и использовали каннабис с 1 января 2014 года. Высокие показатели закупок ($\geq 94,2\%$) и употребления ($\geq 92,5\%$) наблюдались и в предыдущих исследованиях [4,5], несмотря на усилия по набору лиц, не употребляющих наркотические средства.

3.2. Анализ данных.

Биномиальный тест (IBM SPSS версия 24) использовался для определения того, значительно ли отличается доля правильных ответов от ожидаемой случайности, то есть 50%. Результаты показывают, что 7 из 10 образцов обнаружены в пропорции, значительно превышающей ожидаемую случайность. Образцы каннабиса в открытой чаше, мешке Ziploc и мешке из HDPE обнаружены со 100% точностью; результаты оказались идентичны для обоих образцов каннабиса. Кроме того, один образец (Mob Boss), представленный в поп-топ банке, был правильно идентифицирован на статистически значимом уровне. Один образец каннабиса, представленный в канистре с откидной крышкой, и оба образца, представленные в герметически закрытом пластиковом вакууме, идентифицированы на уровнях, статистически не отличающихся от случайных.

4. Обсуждение.

Используя исключительно запах, неподготовленные участники смогли с высокой степенью точности идентифицировать камеру для отбора проб, содержащую 5 г. каннабиса, при представлении образца в открытой чашке, в HDPE пакете или в полиэтиленовом пакете для хранения пищевых продуктов. Летучие соединения, высвобождаемые каннабисом, могли распространяться через эти виды упаковки, успешно создавая концентрации в свободном пространстве. В отличие от этого образец каннабиса не может быть надежно идентифицирован при его упаковке в пластиковый контейнер с двойным вакуумом. Этот метод упаковки ограничивает выброс летучих веществ каннабиса до степени снижения точности обонятельной детекции до вероятностных уровней. Результаты для поп-топ банок, обычно используемых в качестве упаковки для розничных продаж каннабиса в лицензированных аптеках, были неоднозначными. В частности, один образец определен с высокой степенью точности (правильность 95%), другой - со степенью точности, не отличающейся от случайной. Исследователи не смогли объяснить это различие,

предположив, что изменчивость в производственном процессе связана с тем, что некоторые банки были оставлены с неплотно прилегающими крышками в отличие от других.

В анализируемом эксперименте использовались камеры для отбора проб запаха объемом 2 американских галлона (7,6 л.). Вероятно, что открытый образец каннабиса, а также образцы, помещенные в полиэтиленовый пакет HDPE и полиэтиленовый пакет, могут распространять достаточное количество летучих веществ, чтобы обеспечить точное обнаружение в замкнутом пространстве большого объема без других физических барьеров (см. п. 5 «Выводы»). И наоборот, неспособность участников точно определить запах конопли в камерах для отбора проб подразумевает, что задача будет сложной в более замкнутом пространстве, например, в автомобиле.

5. Выводы.

В 2004 Р.Л. Доти (R.L. Doty) пытался определить: «может ли группа мужчин и женщин отличать запах упакованной марихуаны от запаха сопоставимого источника» [6]. В одной из частей исследования испытуемым с завязанными глазами были представлены два пластиковых мешка для мусора: один содержал пять 1-фунтовых пакетов с «прессованной и обработанной мексиканской марихуаной», другой - аналогично связанными измельченными газетами. Их задачей было указать сумку, содержащую запах марихуаны. Девять участников единогласно выбрали мешок, содержащий марихуану (статистически значимый результат). Настоящее исследование расширяет и дополняет проведенное Р.Л. Доти (R.L. Doty) исследование, рассматривая вопрос, насколько точно люди могут детектировать запах конопли, когда последняя находится в различных типах упаковки.

Результаты показывают, что упаковка, которой мы пользуемся в повседневной жизни: мешки HDPE и полиэтиленовые мешки для хранения пищевых продуктов, была неэффективна для ограничения распространения аромата из высушенного цветка конопли. Однако пакеты с двойным вакуумным уплотнением уменьшали распространение запаха каннабиса до уровня, при котором его обнаружение было не лучше, чем случайная детекция.

Однако есть предостережение, касающееся данных результатов: почти безупречное обнаружение запаха каннабиса сквозь вещевые пакеты и пакеты для хранения пищевых продуктов является специфичными для установленных лабораторных условий, поэтому они могут не совпадать с результатами, полученными в реальных условиях, что связано с большим объемом воздуха и физическим разделением помещений для хранения. Например, Р.Л. Доти (R.L. Doty) [6] также рассмотрена возможность детекции запаха каннабиса в пассажирском отделении автомобиля при его нахождении в багажнике. В таких обстоятельствах образец каннабиса - тот же самый, который был обнаружен без ошибок, когда его выявили из мешка для мусора - установлен с частотой, не превышающей вероятность. Таким образом, аромат, легко выявляемый в близком диапазоне, может не обнаружиться в связи с наличием диффузии и большим воздушным пространством. Кроме того, диллюция в виде диффузии в большее физическое пространство может изменить характер смеси запахов: относительно воспринимаемая интенсивность каждого молекулярного компонента изменяется с концентрацией в соответствии с уникальными психофизическими функциями. Таким образом, возможно, что запах каннабиса, если он

достаточно разбавлен, может оставаться обнаруживаемым в качестве запаха, но не может быть точно определен как каннабис.

Другое ограничение исследования состоит в том, что исследовался запах конопли в отсутствие конкурирующих запахов окружающей среды. В реальных условиях в салоне автомобиля могут присутствовать несвязанные запахи: освежители воздуха, контейнеры для фаст-фуда, табак, табачный дым, духи и ароматические аэрозоли для тела. Действительно, некоторые из этих запахов используются водителями и пассажирами для маскировки запаха конопли. Исследования обонятельной психофизики показали, что наблюдателям трудно распознать отдельные компоненты из смеси трех и более запахов [18]. Способность наблюдателей-людей избирательно обнаруживать запах конопли на фоне посторонних запахов требует дальнейшего изучения.

Обнаружение запаха каннабиса через упаковку связано с двумя факторами: выделением летучих веществ из растительного материала и диффузией соединений через упаковочный барьер. Терпены обычно рассматриваются в качестве ключевой физической основы запаха каннабиса. Они являются наиболее распространенными летучими веществами у зрелых растений и сухих цветов [8, 9]. Они производятся в таких количествах, что средства для культивирования каннабиса могут способствовать увеличению региональных концентраций озона [10, 11]. Существуют значительные различия в содержании терпенов между штаммами, но относительно небольшое количество этих соединений обнаруживается неоднократно [8]. Несмотря на то, что запах неофициально использовался для отслеживания микробиологического загрязнения смолы каннабиса [12], комбинированные аналитические и сенсорные исследования, необходимые для идентификации основных ароматических соединений в каннабисе (например, газовая хроматография-ольфактометрия), еще не опубликованы. Важно отметить, что относительное содержание терпена не коррелирует с его обонятельным воздействием [9, 13].

Распространение летучих растительных соединений через упаковочные материалы представляет интерес для специалистов-химиков, и в ходе таких исследований изучены некоторые из терпенов, найденных в каннабисе. Лимонен, например, диффундирует через термосвариваемые пленки, такие как полиэтилен сверхнизкой плотности и модифицированный полиэтилентерефталат [14], а также через картонные коробки с острым верхом, содержащие охлажденный апельсиновый сок [15]. Продемонстрировано, что линалоол и эвкалиптол диффундируют через различные полимерные пленки, включая полиэтилен низкой плотности, полипропилен, нейлон и металлизированный полиэтилентерефталат (МРЕТ) [16]. Скорость диффузии этих терпенов варьируется в зависимости от типа пластика. Способность основных летучих ароматизаторов каннабиса доставлять узнаваемый запах каннабиса вне пластиковой упаковки заслуживает дальнейшего изучения.

Исследователи использовали небольшие корпуса для захвата летучих компонентов в свободном пространстве из образцов высушенного цветка конопли в граммах. Корпуса аналогичного масштаба использовались для расчета интенсивности выбросов терпенов из живых растений каннабиса [17]. Предложенный исследователями метод содержит полезный

подход к моделированию рассеивания аромата конопли внутри (и/из) замкнутого пространства, такого как внутренняя часть автомобиля. Многие уголовные дела, основанные на «доктрине запаха», касаются легковых или грузовых автомобилей [2].

Распространение запаха от промышленной марихуаны растет, то есть большое внутреннее пространство, содержащее массово распределенные источники запаха, потребует другого подхода.

Интерпретация «доктрины запаха» затруднена в штатах, где легализовано хранение небольшого количества каннабиса или хранение лицами, имеющими медицинские показания для приобретения марихуаны. В этих случаях присутствие запаха каннабиса само по себе не означает преступную деятельность. Это поднимает вопрос о том, можно ли оценить количество каннабиса только посредством обонятельной детекции [3]. То, что существуют статистически определенные пределы концентрации, при которой может быть обнаружен данный запах, является основным принципом сенсорной психофизики, и тот, который ставит под сомнение предположение, что когда присутствует конопля, ее запах всегда может быть обнаружен [6].

Отмечается, что «доктрина запаха» не подразумевает однозначную зависимость от восприятия запаха, и что она должна сопровождаться признанием того, что существуют пределы обнаружения любого запаха, к примеру, запах контрабанды должен быть характерным, сильным и стойким [1]. Учитывая результаты исследования, поиски, основанные на запахах, когда материал запечатан в вакуумную упаковку в один или несколько слоев пластика, могут выходить за пределы сферы надежности.

References:

1. Sprow M.A. Wake up and smell the contraband: Why courts that do not find probable cause based on odor alone are wrong // *Wm. & Mary L. Rev.* 42 (2000-2001). P. 289-318.
2. Mandiberg S.F. Marijuana prohibition and the shrinking of the Fourth Amendment // *McGeorge L. Rev.* 43 (2012). P. 23-51.
3. Hoxsie M.P. Probable cause: Is the “plain-smell” doctrine still valid in Arizona after the AMMA? // *Ariz. L. Rev.* 57 (2015). P. 1139-1161.
4. Gilbert A.N., DiVerdi J.A. Consumer perceptions of strain differences in Cannabis aroma // *PLoS ONE* 13 (2018) // URL: e0192247, doi: 10.1371/journal.pone.0192247 (дата обращения: 08.04.2020).
5. Gilbert A.N., DiVerdi J.A. Use of rating scales versus check-all-that-apply ballots in quantifying strain-specific Cannabis aroma, *J. Sensory Studies* (2019) // URL: e12499, DOI: 10.1111/joss.12499 (дата обращения: 08.04.2020).
6. Doty R.L., Wudarski T., Marshall D.A., Hastings L. Marijuana odor perception: Studies modeled from probable cause cases // *Law Hum. Behav.* 28. 2004. P. 223-233.
7. State of Kansas v. Lawrence C. Hubbard, Case No. 113,888 Kansas Supreme Court, December 7, 2018.

8. Booth J.K., Bohlmann J., Terpenes in *Cannabis sativa* – From plant genome to humans, *Plant Sci.* **284** (2019) 67-72 // URL: <https://doi.org/10.1016/j.plantsci.2019.03.022> (дата обращения: 08.04.2020).
9. Rice S., Koziel J.A. Characterizing the smell of marijuana by odor impact of volatile compounds: an application of simultaneous chemical and sensory analysis, *PLoS ONE* **10** (2015a) // URL: e0144160, doi:10.1371/journal.pone.0144160 (дата обращения: 08.04.2020).
10. Plautz J. Growth of legal pot farms drives smog worries, *Science* **363** (2019) 329 // URL: DOI: 10.1126/science.363.6425.329 (дата обращения: 08.04.2020).
11. Wang C-T., Wiedinmyer C., Ashworth K., Harley P.C., Ortega J., Rasool Q. Z., Vizuete W. Potential regional air quality impacts of cannabis cultivation facilities in Denver, Colorado, *Atmos. Chem. Phys.* **2019** // URL: <https://doi.org/10.5194/acp-2019-479> (дата обращения: 08.04.2020).
12. Pérez-Moreno M., Pérez-Lloret P., González-Soriano J., Santos-Álvarez I. Cannabis resin in the region of Madrid: Adulteration and contamination, *Forensic Sci. Int.* **298** (2019) 34-38 // URL: <https://doi.org/10.1016/j.forsciint.2019.02.049> (дата обращения: 08.04.2020).
13. Rice S., Koziel J.A. The relationship between chemical concentration and odor activity value explains the inconsistency in making a comprehensive surrogate scent training tool representative of illicit drugs, *Forensic Sci. Int.* **257** (2015b) 257-270 // URL: <http://dx.doi.org/10.1016/j.forsciint.2015.02.027> (дата обращения: 08.04.2020).
14. Hernandez-Muñoz P., Catalá R., Gavara R. Effect of sorbed oil on food aroma loss through packaging materials, *J. Agric. Food Chem.* **47** (1999) 4370-4374 // URL: <https://pubs.acs.org/doi/10.1021/jf9901791> (дата обращения: 08.04.2020).
15. Aoki R., Tokuda A., Shigemura Y., Mineki M., Sato Y. Aroma leakage from orange juice packed in gable-top paper containers for chilled distribution, *Shokuhin Eiseigaku Zasshi* **58** (2017) 229-233 // URL: doi: 10.3358/shokueishi.58.229. PMID: 29081459 (дата обращения: 08.04.2020).
16. Leelaphiwat P., Auras R.A., Burgess G.J., Harte J.B., Chonhenchob V. Preliminary quantification of the permeability, solubility and diffusion coefficients of major aroma compounds present in herbs through various plastic packaging materials. *J. Sci. Food Agric.* **98** (2018) // URL: 1545-1553, doi: 10.1002/jsfa.8626 (дата обращения: 08.04.2020).
17. Wang C-T., Wiedinmyer C., Ashworth K., Harley P.C., Ortega J., Leaf W. Vizuete enclosure measurements for determining volatile organic compound emission capacity from *Cannabis* spp., *Atmos. Environ.* **199** (2019a) 80-87 // URL: <https://doi.org/10.1016/j.atmosenv.2018.10.049> (дата обращения: 08.04.2020).
18. Laing D.G., Francis G.W. The capacity of humans to identify odors in mixtures, *Physiol. Behav.* **46** (1989) 809-814 // URL: <https://www.sciencedirect.com/science/article/abs/pii/0031938489900413> (дата обращения: 08.04.2020).

19. Gilberta A.N., DiVerdi J.A. Human Olfactory Detection of Packaged Cannabis // Science & Justice. Vol. 60. Iss. 2. 2020. P. 169-172.

Artur G. Holeyvchuk, Andrey V. Uvarov

PROBLEMS OF ODOROLOGICAL DETECTION OF SMELL TRACES OF CANNABIS: USA EXPERIENCE

Olfactory detection of cannabis aroma by police officers can be the basis for warrantless searches of motor vehicles in many jurisdictions in the United States. The odor source in these cases is often dried cannabis flower contained in various casual wrappings as well as in more elaborate packaging. Here we investigate whether packaging format alters the detectability of the cannabis. Two cannabis strains and five packaging formats were evaluated. Untrained observers were presented with two containers and asked to identify, based only on smell, the container that held a sample of packaged cannabis (the other container held identical, but empty, packaging material). The results showed that open and casually packaged cannabis was identified with high accuracy, while material packaged in doubly vacuum-sealed plastic was correctly identified at rates no different from chance. The results may help address issues involving the detectability of cannabis aroma in law enforcement and other scenarios.

Keywords: cannabis; odor detection; olfactory ability; scent; drug detection.

Сведения об авторах:

Холевчук Артур Георгиевич, ФГБОУ ВО «Кубанский государственный университет», филиал в г. Новороссийске, доцент кафедры гуманитарных дисциплин, кандидат юридических наук

Адрес электронной почты: aholevchuk@mail.ru

Уваров Андрей Владимирович, ФГБОУ ВО «Кубанский государственный университет», филиал в г. Новороссийске, студент 4-го курса юридического факультета

Адрес электронной почты: andryuha.uvarov.1999@mail.ru

About the authors:

Artur G. Holeyvchuk, Kuban State University Branch in Novorossiysk, Associate professor of humanitarian disciplines, Candidate of Sciences (Law).

E-mail: aholevchuk@mail.ru

Andrey V. Uvarov, Kuban State University Branch in Novorossiysk, fourth year student of law faculty.

E-mail: andryuha.uvarov.1999@mail.ru

МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ТЕОРИЯ И ПРАКТИКА СУДЕБНОЙ ЭКСПЕРТИЗЫ В СОВРЕМЕННЫХ УСЛОВИЯХ»

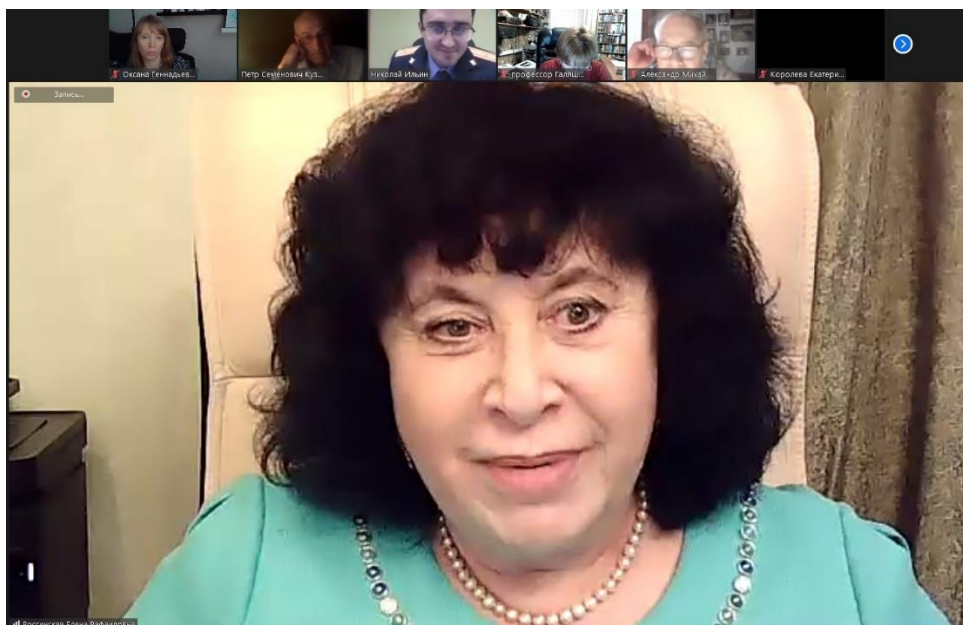
28-29 января 2021 года прошла международная научно-практическая конференция «Теория и практика судебной экспертизы в современных условиях». Конференция проводилась в онлайн-формате на платформе Zoom и собрала около трехсот участников и слушателей.

28 января в рамках Пленарного заседания прозвучали приветственные обращения гостей конференции и интересные доклады на актуальные для науки и практики темы. Так, с приветственным словом к участникам конференции обратилась проректор Университета имени О.Е. Кутафина (МГЮА), д.ю.н., профессор Елена Юрьевна Грачева. Она подчеркнула, что организаторам этой конференции всегда удастся найти интересную тематику, притягивающую ученых, которых волнуют проблемы судебной экспертизы, а также авторитетный уровень проводимой конференции и ее высокую практическую и теоретическую значимость.



Директор Института судебных экспертиз, заведующий кафедрой судебных экспертиз Университета имени О.Е. Кутафина (МГЮА), д.ю.н., профессор Елена Рафаиловна Россинская в своем докладе «Учение о цифровизации судебно-экспертной деятельности в системе частных теорий судебной экспертологии», подготовленном при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003, представила основные положения новой частной теории экспертологии – цифровизации судебно-экспертной

деятельности, привела дефиниции предмет и объекты теории цифровизации судебно-экспертной деятельности, а также систему данной частной теории.



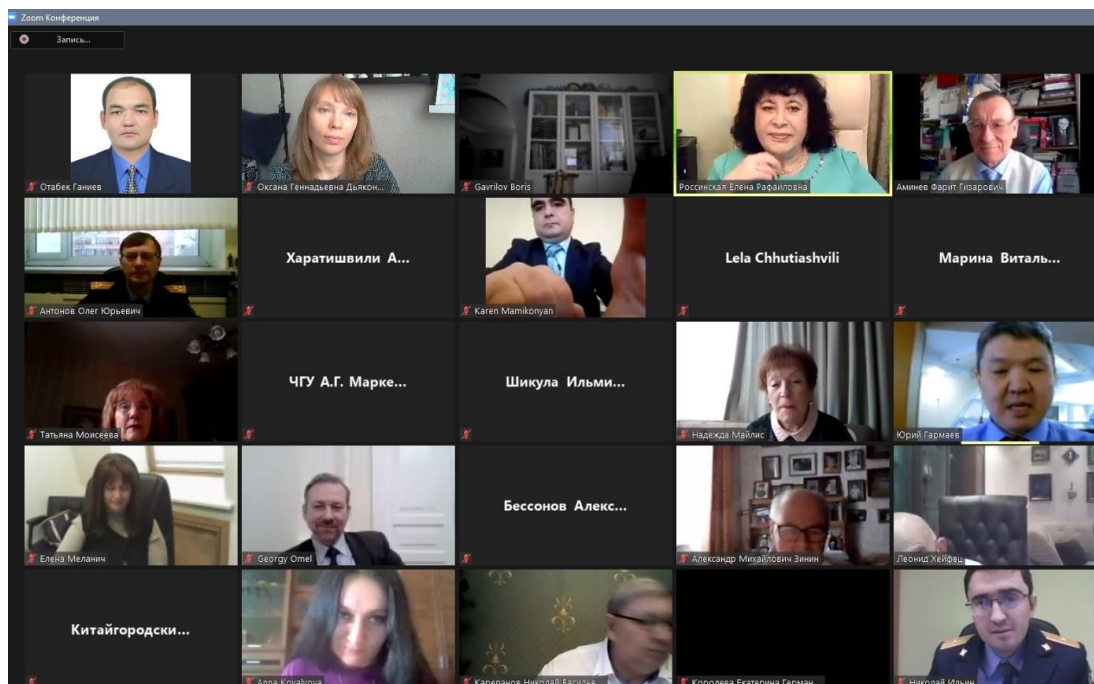
Первый заместитель директора Российского федерального центра судебных экспертиз при Минюсте России, д.ю.н., профессор Александр Иванович Усов в приветственном слове обратил внимание на происходящие в нашем обществе «цифровые трансформации», которые повлияли на появление в рамках судебной экспертологии самостоятельной теории, о которой говорила профессор Е.Р. Россинская, новых объектов судебных экспертов, необходимости выработки новых подходов к их исследованию.



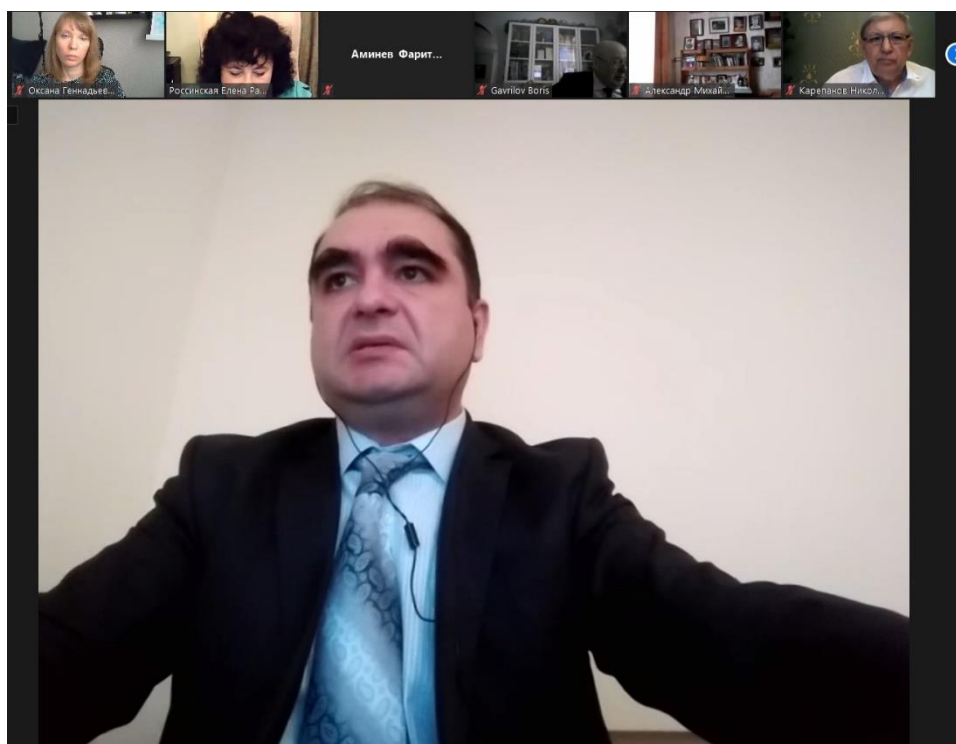
Совместный доклад на тему «Методологические основы современного научного анализа судебно-экспертной деятельности» с предлагаемым решением поставленной проблематики представили профессор кафедры криминалистики Института права Башкирского государственного университета, д.ю.н., профессор Фарит Гизарович Аминев

ТЕОРИЯ И ПРАКТИКА СУДЕБНОЙ ЭКСПЕРТИЗЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

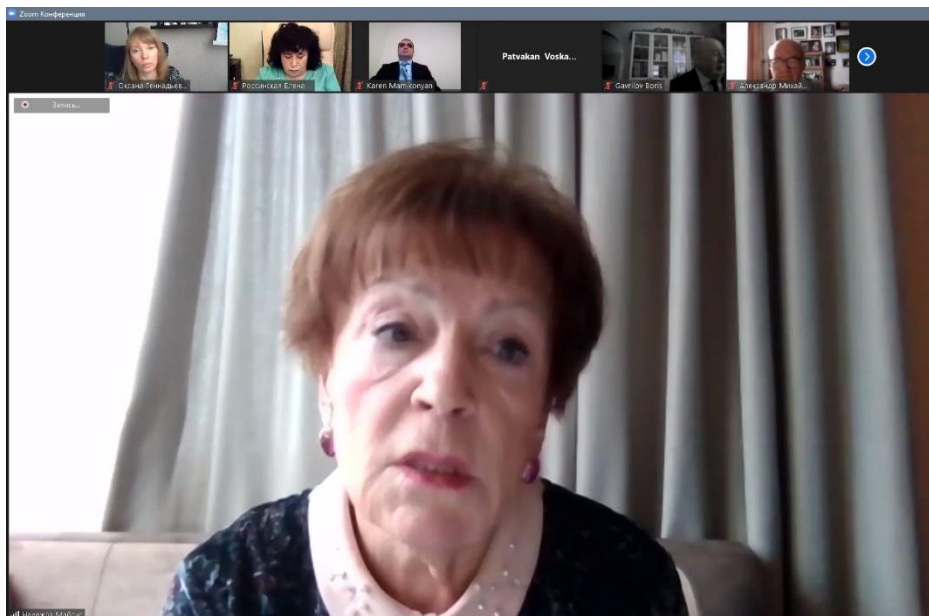
и профессор кафедры криминалистики Кубанского государственного аграрного университета имени И.Т. Трубилина д.ю.н., профессор Юрий Петрович Гармаев.



Начальник отдела координации научных исследований и технического апробирования Национального бюро экспертиз Национальной академии наук Республики Армения, эксперт отдела финансово-экономических и бухгалтерских экспертиз, доцент кафедры финансов Армянского государственного экономического университета, к.э.н. Карен Оганесович Мамиконян осветил проблемы назначения и производства финансово-экономической экспертизы при банкротстве юридических лиц.

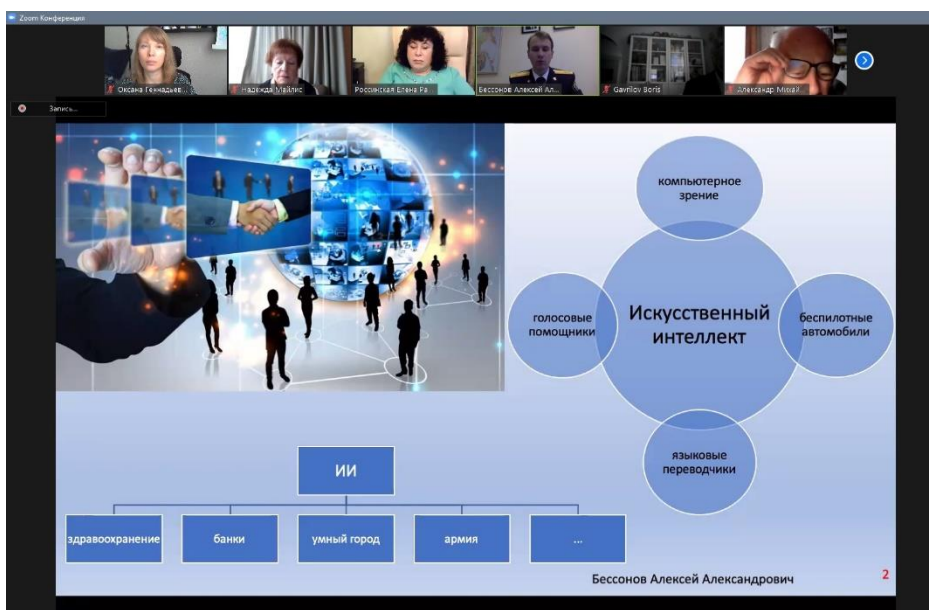


О роли языка в судебной экспертизе на современном этапе ее развития, об унификации языка судебной экспертизы и стандартизации понятий в судебно-экспертной деятельности рассказала профессор кафедры оружиеведения и трасологии УНК судебных экспертиз Московского университета МВД России имени В.Я. Кикотя, д.ю.н., профессор Надежда Павловна Майлис. Как верно отметила Н.П. Майлис, «интеграция знаний носит многоуровневый характер и в экспертных исследованиях используются комплексно физические, химические, биологические и другие методы исследования.



При этом могут быть применены и технические средства, разработанные другой наукой, что принесет и новые термины в судебную экспертизу». Кроме того, в своем докладе Н.П. Майлис подняла ряд проблем, связанных со спецификой экспертной коммуникации при производстве комплексных и комиссионных экспертиз.

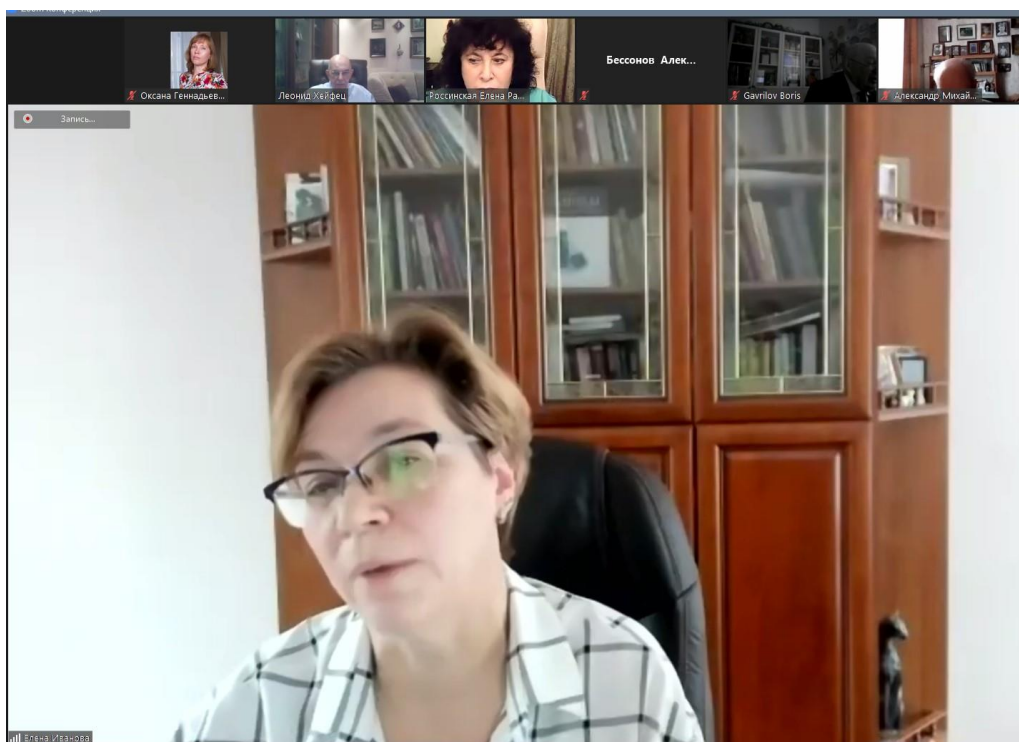
Профессор кафедры криминалистики Московской академии Следственного комитета РФ, д.ю.н., доцент Бессонов Алексей Александрович в своем докладе о современном



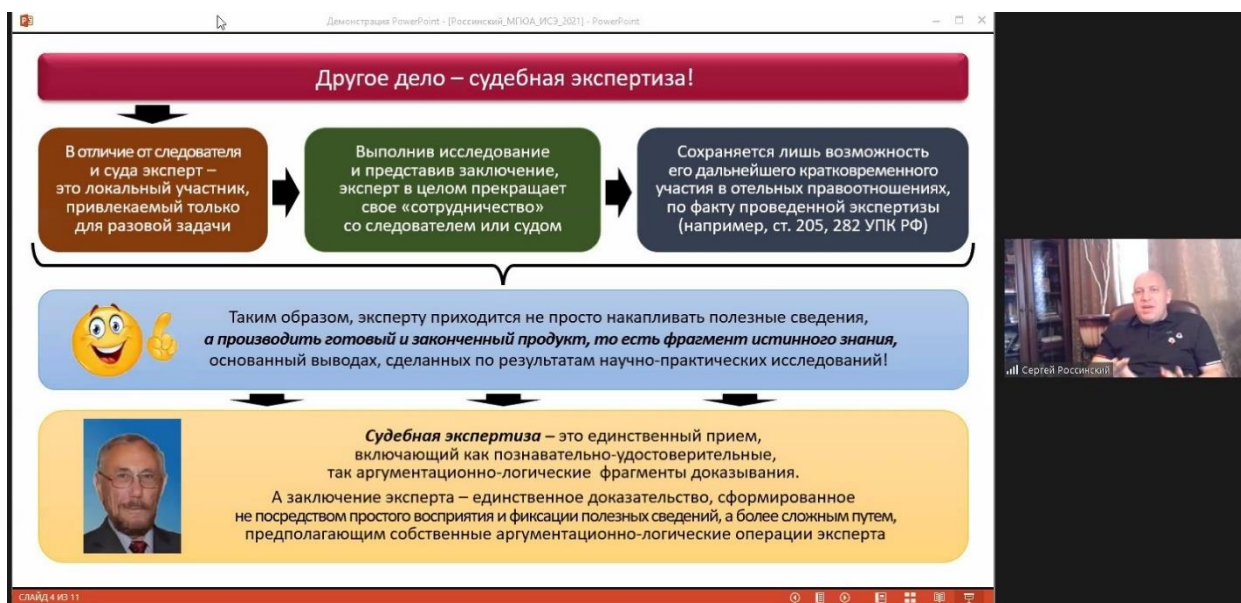
ТЕОРИЯ И ПРАКТИКА СУДЕБНОЙ ЭКСПЕРТИЗЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

состоянии и перспективах использования искусственного интеллекта в судебной экспертизе указал на ключевые препятствия активной интеграции искусственного интеллекта в судебную экспертизу, а также отметил проблемы его использования в судебной экспертизе в свете действующей Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях.

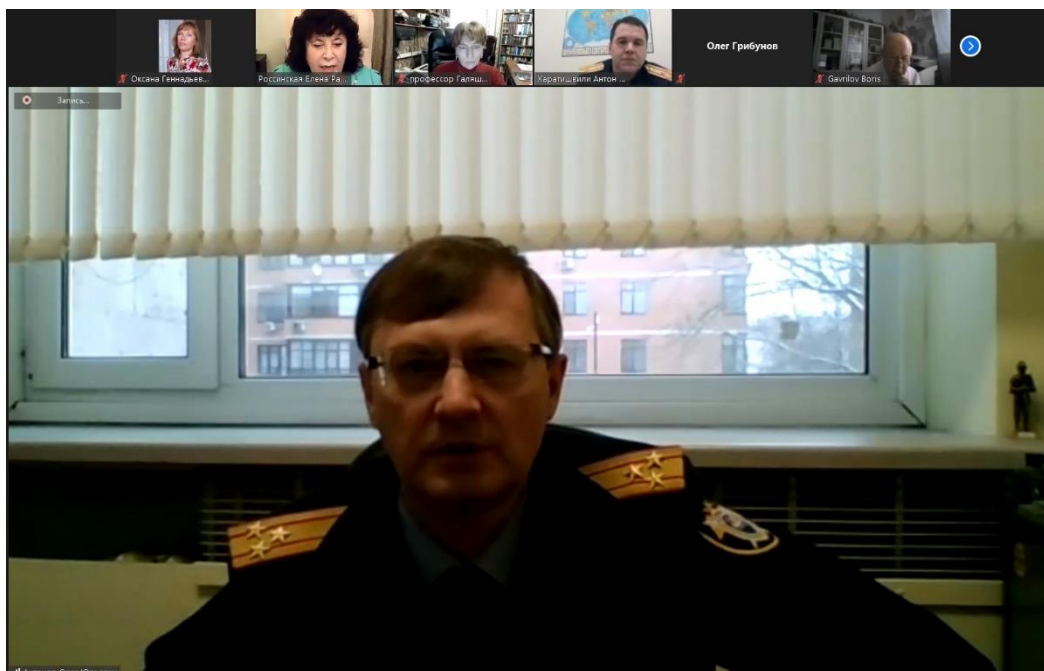
Заведующий кафедрой криминалистики и уголовного процесса Государственного социально-гуманитарного университета, д.ю.н., доцент Елена Вячеславовна Иванова, рассказала о проблемах, возникающих при определении компетенции «негосударственного» эксперта, о так называемых «профессиональных» и «непрофессиональных» экспертах, которые не осуществляют судебно-экспертную деятельность на профессиональной основе, а также о проблемах обучения и переподготовки таких экспертов различными негосударственными организациями.



Оживленную дискуссию вызвал доклад профессора кафедры уголовно-процессуального права Университета имени О.Е. Кутафина (МГЮА), д.ю.н., доцента Россинского Сергея Борисовича на тему «И все-таки он научный судья! (О роли эксперта в доказывании по уголовному делу)». С.Б. Россинский поднял ряд проблем, связанных с оценкой заключения эксперта, отметил, что «должное внимание его глубокому смыслу и подлинному значению» правоприменители уделяют мало, а также привел аргументы противников и сторонников подхода «эксперт – научный судья», сделав в итоге вывод о необходимости «изменении доктринальных и законодательных подходов к роли эксперта как субъекта доказывания в уголовном судопроизводстве, а именно о перспективах его наделения полномочиями научного судьи», а также о «пересмотре государственной политики в отношении организации и кадрового обеспечения судебно-экспертной деятельности».



Актуальную тематику в своем докладе «Теоретические проблемы судебной экспертологии в условиях интеграции и дифференциации научного знания» поднял декан факультета подготовки криминалистов Московской академии Следственного комитета РФ, д.ю.н., доцент Антонов Олег Юрьевич. Отметив дифференциацию научного знания – криминалистики и судебной экспертологии – он выделил интегративные направления развития обеих наук и подчеркнул необходимость развития «формируемой Е.Р. Россинской теории информационно-компьютерного обеспечения криминалистической деятельности в условиях цифровизации».



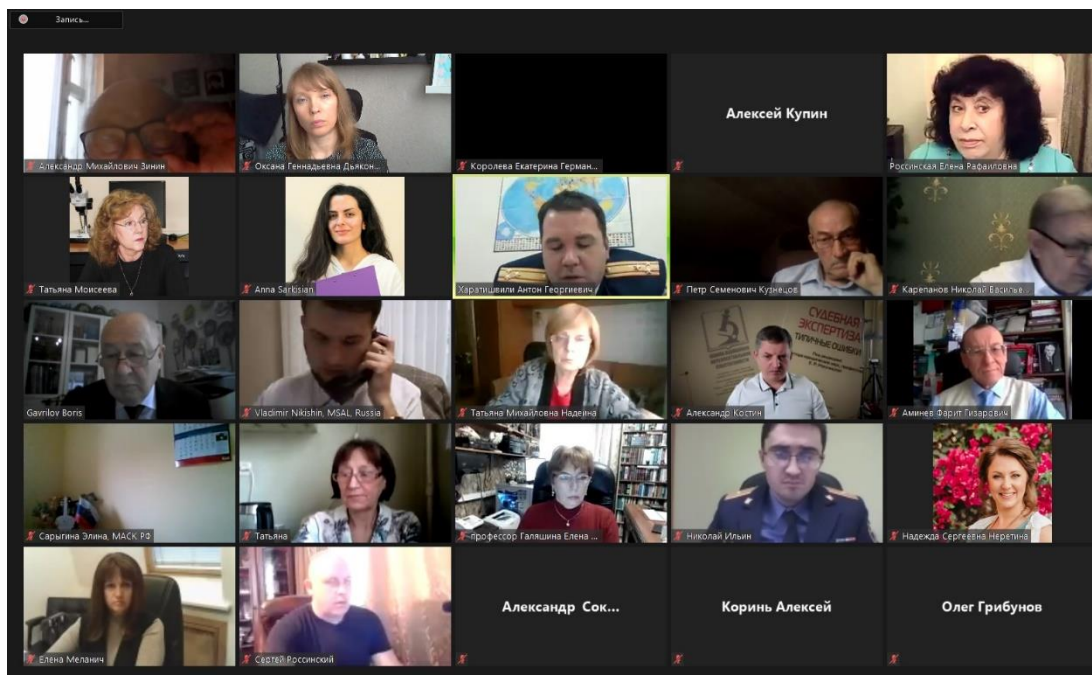
Заведующий кафедрой судебных экспертиз и криминалистики Российского государственного университета правосудия, д.ю.н., профессор Татьяна Федоровна Моисеева предложила акцентировать внимание на проблемах и перспективах использования

ТЕОРИЯ И ПРАКТИКА СУДЕБНОЙ ЭКСПЕРТИЗЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

специальных знаний в области психологии в судопроизводстве. Она отметила различия в деятельности специалиста и эксперта, применяющих знания в области психологии, остановилась на проблемах использования результатов психофизиологических исследований и подчеркнула «необходимость развития методологического обеспечения таких исследований, путем разработки методик исследования, основанных на единых методических принципах, репрезентативной экспериментальной базе и прошедших верификацию».



С докладом о процессуальном статусе ведомственного эксперта выступил заведующий кафедрой уголовного процесса Санкт-Петербургской академии Следственного комитета РФ, к.ю.н., доцент Антон Георгиевич Харатишвили, обративший внимание на проблему обеспечения независимости ведомственных судебных экспертов.



Профессор кафедры управления органами расследования преступлений Академии управления МВД России, заслуженный юрист РФ, заслуженный деятель науки РФ, д.ю.н., профессор Гаврилов Борис Яковлевич в своем докладе подробно остановился на правовых и организационных проблемах судебно-экспертной деятельности на стадии возбуждения уголовного дела, поднял вопросы обязательного назначения судебных экспертиз по ряду дел, проведения специалистом исследований до возбуждения уголовного дела, совершенствования уголовно-процессуального законодательства об использовании специальных знаний на этапе проверки заявления, сообщения о преступлении.



Профессор кафедры судебных экспертиз Университета имени О.Е. Кутафина (МГЮА), д.ю.н., д.филол.н., академик РАЕН, профессор Елена Игоревна Галяшина выступила с докладом на тему «Использование специальных знаний для обеспечения мировоззренческой медиа безопасности», подготовленным при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00190.



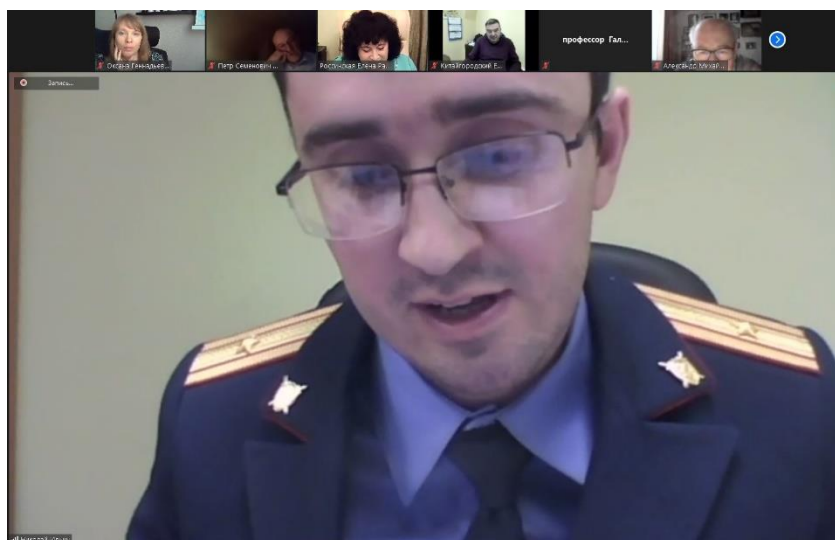
ТЕОРИЯ И ПРАКТИКА СУДЕБНОЙ ЭКСПЕРТИЗЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

В докладе Е.И. Галяшина подчеркнута существенные угрозы информационной безопасности, возникающие в связи с расширением возможностей манипулирования сознанием человека за счет формирования вокруг него индивидуального виртуального информационного пространства, предложила дефиницию «мировоззренческая медиабезопасность» как вида деятельности, а также подчеркнула роль лингвистических специальных знаний в процессе распознавания деструктивной сущности способов и видов информационно-психологического воздействия и оценке их угроз для индивидуального и общественного сознания.

С докладом о проблемах нормативно-правового регулирования геномной регистрации и использования результатов ДНК-анализа в раскрытии и расследовании преступлений выступил заместитель начальника института (по научной работе) Восточно-Сибирского института МВД России, д.ю.н., профессор Олег Павлович Грибунов. Он обратил внимание слушателей на необходимость расширения перечня субъектов, подлежащих обязательной геномной регистрации.

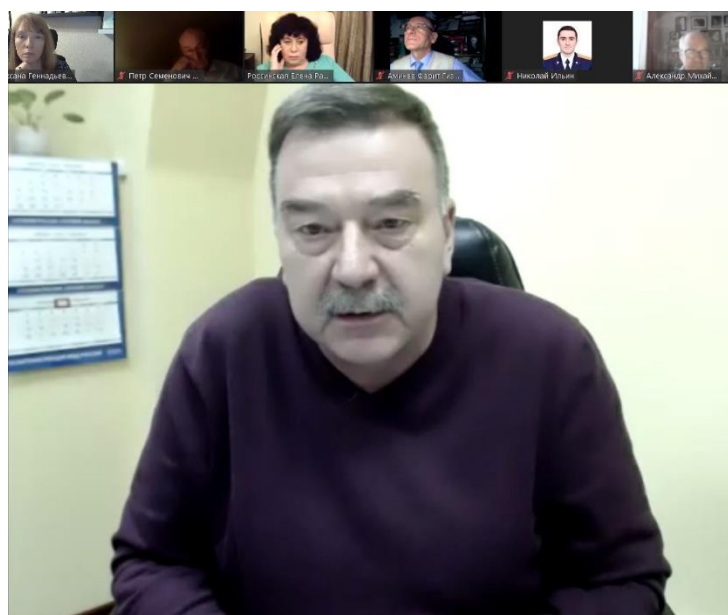


Николай Николаевич Ильин, и.о. заведующего кафедрой судебно-экспертной и оперативно-разыскной деятельности Московской академии Следственного комитета РФ, к.ю.н. предложил обсудить вопросы компетентности субъектов по производству транспортно-технических судебных экспертиз.

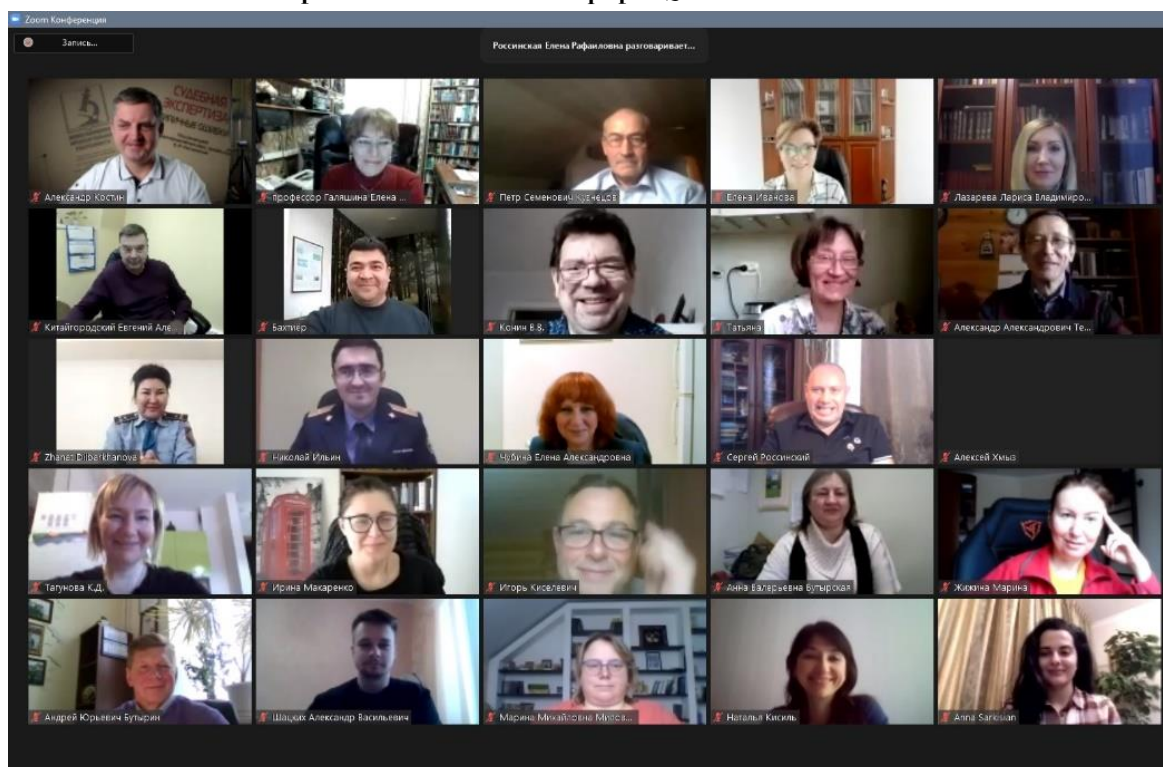


Особое внимание Н.Н. Ильин уделил вопросу негосударственных судебных экспертов и экспертным учреждениям, наиболее востребованным для производства экспертиз обозначенного вида.

После представления основных докладов присутствовавших участников на Пленарном заседании генеральный директор Палаты судебных экспертов имени Ю.Г. Корухова (СУДЭК) Евгений Александрович Китайгородский представил для открытого обсуждения профессиональный стандарт «Специалист в области судебной экспертизы», подготовленный Палатой судебных экспертов имени Ю.Г. Корухова совместно с РФЦСЭ при Минюсте России, АНО «СОДЭКС МГЮА имени О.Е. Кутафина», НИИ безопасности движения УГЛТУ, а также Общественным советом по СЭД в Республике Башкортостан¹.

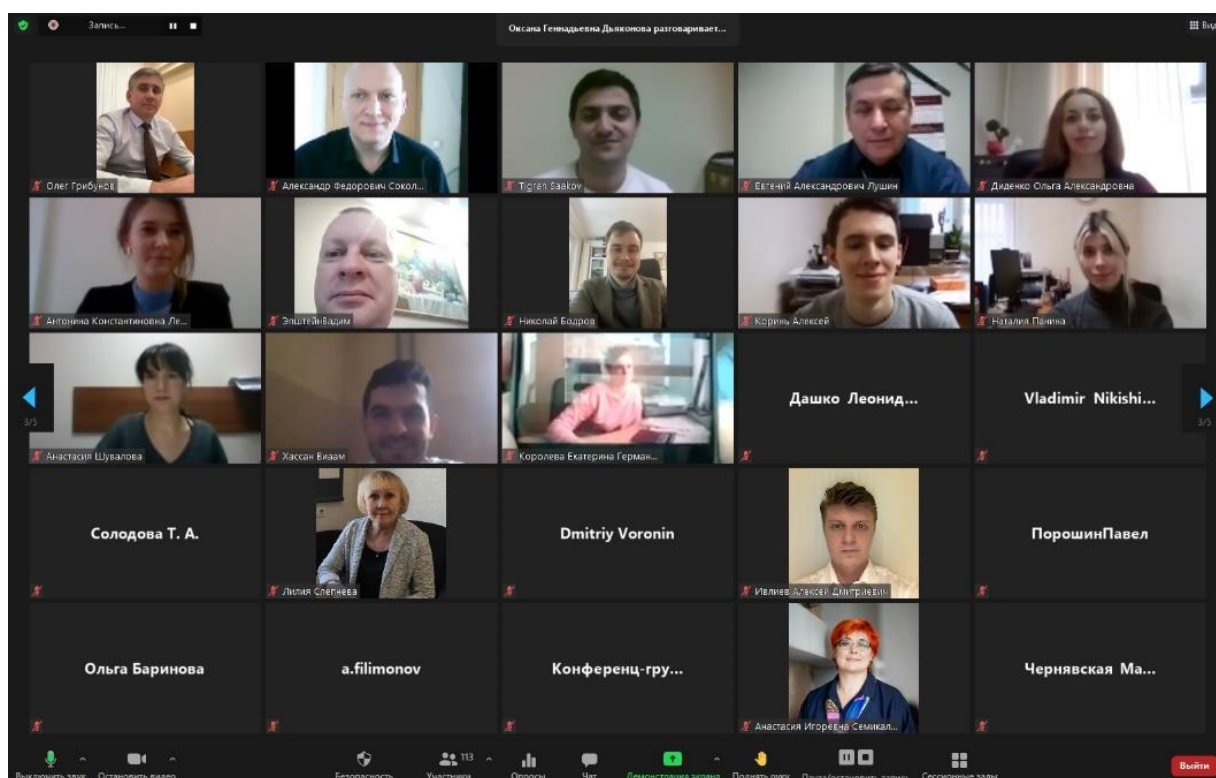
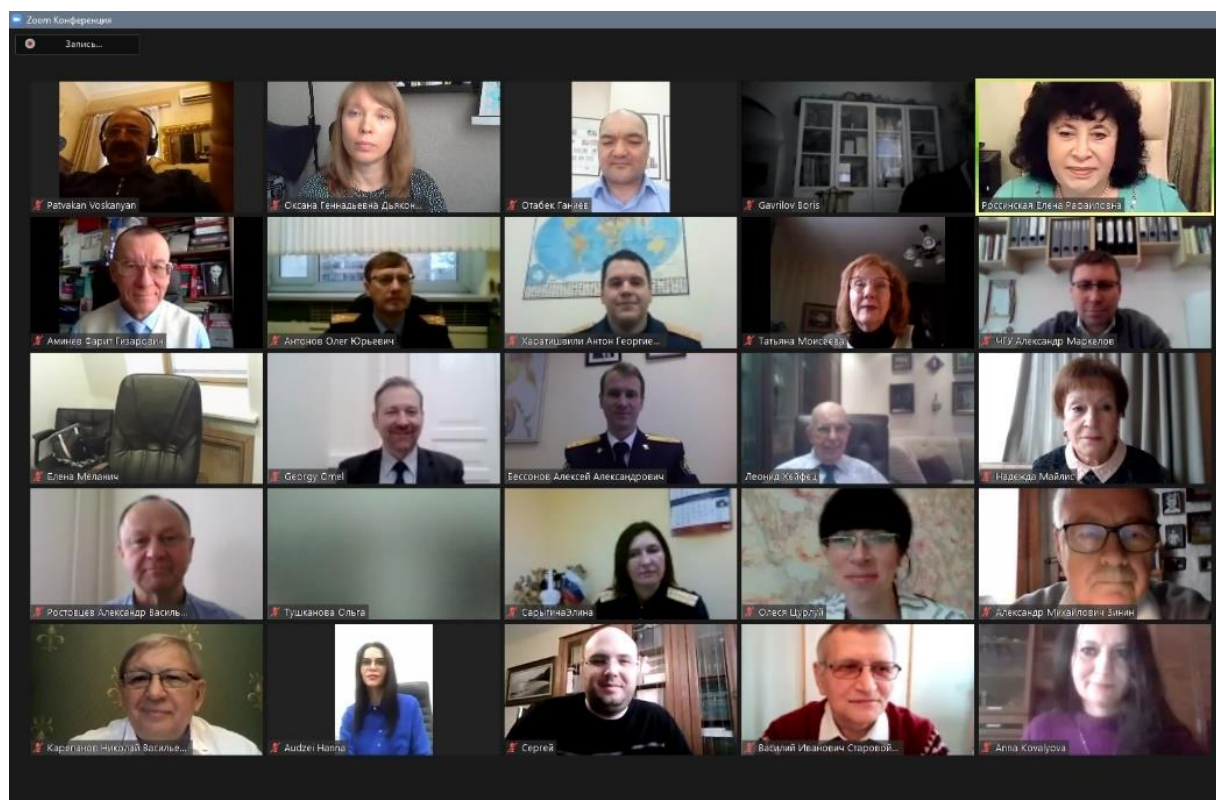


Участники Пленарного заседания конференции:



¹ С текстом документа можно ознакомиться: [Электронный ресурс] URL: <https://www.sudex.ru/profstandart/2646233> (дата обращения: 20.01.2021).

ТЕОРИЯ И ПРАКТИКА СУДЕБНОЙ ЭКСПЕРТИЗЫ В СОВРЕМЕННЫХ УСЛОВИЯХ



29 января 2021 года конференция проходила в рамках тематических секций по следующим направлениям:

Секция № 1 Теоретические, правовые и организационные проблемы судебной экспертологии в современных условиях.

Секция № 2 Современные проблемы криминалистических экспертиз.

Секция № 3 Современные проблемы судебных инженерно-технических экспертиз.

Секция № 4 Современные проблемы судебных речеведческих экспертиз.

Секция № 5 Современные проблемы судебных экономических экспертиз.

Секция № 6 Проблемы судебно-медицинских, судебно-психиатрических и психологических экспертиз, судебно-биологических экспертиз¹.

В указанных секциях прозвучали интересные доклады и состоялась дискуссия по наиболее острым вопросам и проблемам, возникающим в правоприменении при использовании специальных знаний.

По результатам конференции был опубликован сборник: Теория и практика судебной экспертизы в современных условиях: материалы VIII Международной научно-практической конференции. – Москва: РГ-Пресс, 2021. – 384 с.

Обзор подготовлен к.ю.н., доцентом О.Г. Дьяконовой

¹ Видеозапись Пленарного заседания и секций доступны на официальном You-tube канале кафедры судебных экспертиз МГЮА [Электронный ресурс] URL: https://www.youtube.com/channel/UCQGu7SSllfMN91hxHh_5gQA (дата обращения: 20.01.2021)

Требования для авторов

Тематика журнала «ВестникЪ криминалистики ~ Bulletin of criminalistics»:

Научно-практический журнал «ВестникЪ криминалистики ~ Bulletin of Criminalistics» издается с 1999 года. В журнале публикуются статьи по криминалистике, судебной экспертизе и оперативно-розыскной деятельности, представляющие интерес для практических работников правоохранительных органов, а также адвокатов, судей, преподавателей криминалистики и научных работников.

Журнал распространяется преимущественно по подписке. Подписчиками журнала являются юридические ВУЗы и юридические факультеты России, ближнего и дальнего зарубежья (Белоруссия, Казахстан, Украина, Узбекистан, Литва, Латвия, Эстония, Польша, Словения, Словакия, Сербия), правоохранительные органы России (МВД, Следственный Комитет России), а также ученые и практики.

Порядок направления материалов в редакцию

1. Автор направляет в электронном виде на адрес редакции журнала: author@vesterim.ru **статью и заявку.**

2. Для обеспечения соблюдения законодательства Российской Федерации в сфере авторского права редакция журнала «Вестник криминалистики» предлагает заключить авторский договор на опубликование авторских материалов, который в виде публичной оферты размещен на официальном сайте журнала и на странице журнала «Вестник криминалистики» в социальной сети Facebook (<https://www.facebook.com/VestCrim/>).

Договор считается заключенным после получения редакцией журнала статьи и заявки на опубликование статьи. В заявке приводятся следующие сведения о каждом авторе: данные об авторе (ФИО, дата рождения, место рождения, паспортные данные: серия, №, выдан, код подразделения); адрес места работы; электронный адрес; телефон.

3. Направление статьи и заявки в электронном виде в редакцию журнала является акцептом о заключении с редакцией журнала «Вестник криминалистики» безвозмездного договора об отчуждении исключительного права на Произведение на основании ст.ст.1234, 1285 ГК РФ.

4. Статьи проходят рецензирование в обязательном порядке.

5. Если автором является соискатель ученой степени кандидата юридических наук, следует дополнительно представить сканированную копию рецензии научного руководителя.

6. В случае включения в текст статьи рисунков, графиков, иного иллюстративного материала, автор должен представить в отдельном файле эти иллюстрации с подписями под каждой из них.

Рецензирование рукописей

В журнале осуществляется рецензирование всех представленных для опубликования рукописей. Рецензирование осуществляется квалифицированным специалистом по тематике рецензируемого материала.

Рецензирование осуществляется в течение 45 дней с момента поступления рукописи по электронной почте на адрес редакции журнала.

В рецензии отражается актуальность и проблематика темы исследования, соответствие тематике журнала, адекватность примененных методов исследования, степень научной новизны исследования, практическая значимость, характеристика статьи по стилю, замечания рецензента автору (если имеются), в качестве общего заключения — вывод о рекомендации для опубликования в журнале «Вестник криминалистики».

При наличии замечаний рецензента автору рекомендуется внести исправления в статью в срок до 14 рабочих дней. После устранения замечаний и прохождения повторного рецензирования статья принимается к опубликованию.

Рецензии хранятся в редакции издания в течение 5 лет.

Статьи, опубликованные или принятые к публикации в других изданиях, к публикации в журнале «Вестник криминалистики» не допускаются. Если статья (материал) одновременно направляется в другое издание либо была опубликована ранее, автор обязан сообщить об этом в редакцию.

Статья публикуется в авторской редакции, но в случае превышения объема рукопись может быть сокращена по усмотрению редактора.

Общие требования к рукописям статей

1. Статья принимается в электронном виде в формате MS Word 7.0 и более поздних версий.

2. Текст оформляется через полуторный интервал, кегль шрифта – 14, поля: верхнее, нижнее = 2 см, правое = 3 см, левое = 2 см. Абзацный отступ следует задавать только с помощью функции «ГЛАВНАЯ / АБЗАЦ / ОТСТУПЫ И ИНТЕРВАЛЫ / ПЕРВАЯ СТРОКА» и должен быть равен 1,25 см.

3. Допускается размещение диаграмм в формате Excel, рисунков в формате TIFF или JPEG, с обязательным приведением их в отдельном файле с подписями к каждому рисунку. Рисунки и диаграммы выполняются без заливки в черно-белом варианте.

4. На литературные источники сноски в тексте не размещаются. Оформляются затекстовые библиографические ссылки с размещением номера источника и страницы цитирования в квадратных скобках в соответствии с ГОСТ Р 7.0.5-2008.

Образец оформления библиографической ссылки:

Если делается ссылка на автора и его книгу без цитирования конкретного фрагмента:

В тексте: Общий список справочников по терминологии, охватывающий время не позднее середины XX века, дает работа библиографа И. М. Кауфмана [59].

В затекстовой ссылке: 59. Кауфман И. М. Терминологические словари: библиография. М., 1961.

Если ссылку приводят на конкретный фрагмент текста документа:

В тексте: [10, с. 81]

В затекстовой ссылке: 10. Бердяев Н. А. Смысл истории. М.: Мысль, 1990. 175 с.

5. Объем материала допускается до 30 000 печатных знаков, что соответствует объему до 20 страниц.

Образец оформления Библиографического списка.

Библиографический список:

1. Бердяев Н. А. Смысл истории. М.: Мысль, 1990. 175 с.

2. Кауфман И. М. Терминологические словари: библиография. М., 1961. 419 с.

3. Иванова Е.В., Дьяконова О.Г. Правовые формы судебно-экспертной деятельности в ракурсе проблемы конкурентно-способности // Аубакировские чтения: материалы международной научно-практической конференции (19 февраля 2018 г.). Алматы, 2018. С.144-147.

References:

1. Berdyaev N.A. The meaning of history. M.: Mysl', 1990. 175 p. (In Russ.)

2. Kaufman I.M. Terminological dictionaries: bibliography. M., 1961. 419 p. (In Russ.)

3. Ivanova E.V., Dyakonova O.G. Legal forms of forensic activity in the view of the problem of competitiveness: Aubakirov's readings: materials of the international scientific-practical conference. Almaty, 2018. P.144-147. (In Russ.)

Обратите внимание, что **нормативные и нормативные правовые акты, а также ссылки на Интернет-сайты не выносятся в библиографический список, ссылки на них размещаются в подстрочной сноске!**

6. Все сокращения расшифровываются при первом их упоминании в тексте.

7. На последней странице статья должна быть проставлена подпись автора, подтверждающая, что статья выверена, данные соответствуют действительности.

8. Структурные элементы статьи, подлежащие опубликованию:

1) Заголовок статьи на русском и английском языках;

2) Сведения об авторе: фамилия (полностью), инициалы;

3) Аннотация (Abstract). Представляется на русском и английском языках в количестве от 150-250 слов и должна отражать постановку проблемы исследования, цель работы, результаты исследования и краткий вывод.

4) Ключевые слова (Keywords) – 10-15 слов на русском и английском языках;

5) Текст статьи, включающий: введение, цель работы, материал, обсуждение, выводы.

6) Библиографический список на русском языке и список литературы на английском языке в отношении источников, опубликованных на русском языке (References).

7) Сведения об авторе: фамилия, имя, отчество (полностью), ученая степень, ученое звание, должность, место работы, адрес места работы, адрес электронной почты на русском и английском языках.

Адрес редакции:

author@vestcrim.ru, contact@fact-gsgu.ru

тел.8(499)3933894, 8(916)7174507.

Научное издание

BULLETIN OF CRIMINALISTICS № 1 (77), 2021

*Всероссийский научно-практический журнал
«ВестникЪ криминалистики ~ Bulletin of Criminalistics»*

Ответственный редактор д.ю.н., доцент Е.В. Иванова

Корректор Т.В. Иванова

Подписано в печать 30.03.21. Формат 70х108/16.

Печ. л. 6. Тираж 600 экз. Заказ № 30-03/2021

Отпечатано в ООО «Объединенная Рязанская типография»
390000, г. Рязань, ул. Семинарская, 39

140410, г. Коломна, ул. Зеленая, 30.

Автономная некоммерческая организация «Центр судебных экспертиз
Государственного социально-гуманитарного университета
«ФАКТ»

Издаётся при содействии

ГОУ ВО МО

«Государственный социально-гуманитарный университет»