Мазуров Игорь Евгеньевич. Методика расследования хищений, совершенных с использованием интернет-технологий: диссертация ... кандидата Юридических наук: 12.00.12 / Мазуров Игорь Евгеньевич;[Место защиты: ФГКОУВО Ростовский юридический институт Министерства внутренних дел Российской Федерации], 2017.- 188 с.

**Содержание к диссертации**

Введение

**Глава 1. Криминалистическая характеристика хищений, совершенных с использованием интернет-технологий 12**

1.1. Понятие и общие положения криминалистической характеристики хищений, совершенных с использованием интернет-технологий 12

1.2. Способы совершения и сокрытия хищений, совершенных с использованием интернет-технологий 17

1.3. Личность преступника, совершающего хищения с использованием интернет-технологий 25

1.4. Другие элементы криминалистической характеристики хищений, совершенных с использованием интернет-технологий 29

**Глава 2. Возбуждение уголовного дела, первоначальные и последующие этапы расследования хищений, совершенных с использованием интернет-технологий 42**

2.1. Особенности возбуждения уголовного дела по хищениям, совершенным с использованием интернет-технологий 42

2.2. Особенности первоначального этапа расследования хищений, совершенных с использованием интернет-технологий 52

2.3. Последующий этап расследования хищений, совершенных с использованием интернет-технологий 62

**Глава 3. Особенности тактики следственных действий по делам о хищениях, совершенных с помощью интернет –технологий 70**

3.1. Особенности осмотра места происшествия по делам о хищениях, совершенных с помощью интернет-технологий 70

3.2. Осмотр компьютерных устройств 82

3.3. Осмотр машинного документа в ходе расследования хищений, совершенных с использованием интернет – технологий 90

3.4. Тактика допроса в ходе расследования хищений, связанных с использованием интернет-технологий 94

3.5. Обыск и выемка в ходе расследования по делам о хищениях, совершенных с использованием интернет - технологий 107

3.6. Особенности назначения и производства экспертиз при расследовании хищений, совершенных с использованием интернет-технологий 116

**Глава 4. Предупреждение хищений, совершенных с использованием интернет-технологий 128**

4.1. Причины и факторы, способствующие совершению хищений с использованием интернет-технологий 128

4.2. Общие и специальные меры профилактики хищений, совершенных с использованием интернет-технологий 138

Заключение 160

Список использованной литературы

* [Способы совершения и сокрытия хищений, совершенных с использованием интернет-технологий](http://www.dslib.net/finans-pravo/metodika-rassledovanija-hiwenij-sovershennyh-s-ispolzovaniem-internet-tehnologij.html#7671671)
* [Особенности первоначального этапа расследования хищений, совершенных с использованием интернет-технологий](http://www.dslib.net/finans-pravo/metodika-rassledovanija-hiwenij-sovershennyh-s-ispolzovaniem-internet-tehnologij.html#7671672)
* [Осмотр машинного документа в ходе расследования хищений, совершенных с использованием интернет – технологий](http://www.dslib.net/finans-pravo/metodika-rassledovanija-hiwenij-sovershennyh-s-ispolzovaniem-internet-tehnologij.html#7671673)
* [Общие и специальные меры профилактики хищений, совершенных с использованием интернет-технологий](http://www.dslib.net/finans-pravo/metodika-rassledovanija-hiwenij-sovershennyh-s-ispolzovaniem-internet-tehnologij.html#7671674)

**Введение к работе**

**Актуальность выбора темы диссертационного исследования**. В  
современной России приоритетной задачей является создание

информационного общества на основе широкого внедрения современных интернет-технологий. Одной из определяющих задач на этом направлении является формирование комплексной инфраструктуры оказания электронных услуг населению. Согласно стратегии развития информационного общества, утвержденной Президентом Российской Федерации 7 февраля 2008 г. (№ Пр-212)1, все государственные услуги должны быть переведены в электронный вид уже к 2015 г. Проблема актуальна, имеет научный и практический интерес, поскольку сегодня современные интернет-технологии затрагивают практически все области жизнедеятельности человека.

Развитие современных интернет-технологий и информационного пространства способствует увеличению преступных посягательств, в частности хищений, совершенных с помощью интернет-технологий. Данные ГИАЦ МВД России показывают, что за период с 2008 по 2016 гг. хищений с использованием интернет-технологий было совершено 91509, из которых 61,1% - кражи, 22,3% – мошенничества, 9,1 % – присвоение и растрата, 7,5% -грабежи и разбои.

Согласно Отчету NCR (Norton Cybercrime Report), жертвами хищений, совершенных с помощью интернет-технологий в 2016 г., стали 341 миллион человек. Более 65 % пользователей интернета сталкивались с хищениями, совершенными с помощью интернет-технологий в сети, 21% из них пользовались смартфонами и мобильными телефонами. Ущерб, причиненный пользователям интернета, составил более 412 млрд долларов США. Затраты на восстановление базы данных после действий преступников в области современных интернет-технологий составляют более 300 млн долларов.

1 Российская газета. 2014. 16 февраля.

Данные обстоятельства способствовали созданию Генеральной Ассамблеей ООН комиссии по предотвращению данной категории преступлений.1

Несмотря на масштабы и социальную опасность хищений, совершенных с использованием интернет-технологий, в юридической литературе нет монографических работ, посвященных расследованию и предупреждению данной категории преступлений. Необходимо исследовать данную проблему с использованием современных достижений кибернетики, информатики, криминалистики, психологии, педагогики.

По мнению автора, необходимо создать систему учета хищений, совершенных с использованием интернет-технологий. Несовершенство статистики затрудняет разработку эффективных мер борьбы с данной категорией преступлений. В ходе анализа современной и зарубежной литературы вопросы, посвященные расследованию хищений, совершенных с помощью интернет-технологий, рассмотрены недостаточно и играют огромную роль в борьбе с данной категорией преступлений.

**Цель** диссертационного исследования – разработка комплекса тактико-  
криминалистических рекомендаций, направленных на повышение  
эффективности раскрытия, расследования и предупреждения хищений,  
совершаемых с помощью интернет-технологий. Для реализации данной цели  
разработан комплекс следующих **задач**:

изучение и обобщение нормативной, монографической и иной литературы по криминалистике, уголовному процессу, оперативно-розыскной деятельности, посвященной особенностям расследования хищений денежных средств и информации с помощью интернет-технологий;

определение правовой и тактической сущности хищений с помощью интернет-технологий;

- разработка элементов криминалистической характеристики хищений,  
совершенных с использованием интернет-технологий;

1 Решение 65/230 Генеральной Ассамблеи ООН.

- изучение особенностей возбуждения уголовного дела о хищениях,  
совершенных с использованием интернет-технологий;

- определение специфики тактики первоначальных следственных  
действий по делам о хищениях, совершенных с использованием интернет-  
технологий;

- разработка следственных действий по делам о хищениях, совершенных  
с использованием интернет-технологий на последующем этапе;

- разработка тактико-криминалистических рекомендаций, повышающих  
эффективность процесса предупреждения хищений, совершенных с  
использованием интернет-технологий.

**Объект исследования** – теория и практика расследования хищений с помощью интернет-технологий.

**Предмет** **исследования** – закономерности деятельности

правоохранительных органов в сфере раскрытия, расследования и

предупреждения хищений, совершенных с помощью интернет-технологий.

**Методологическую основу** диссертационного исследования составляет совокупность общих и частных методов научного познания, в первую очередь, -положения диалектического учения о всеобщей связи и развитии. При выполнении диссертационного исследования применялись иные общенаучные и частнонаучные методы познания изучаемых явлений: системно-структурный, формально-логический, логико-юридический, исторический, сравнительно-правовой, функциональный, индуктивный и дедуктивный, анализ и синтез, аналогия, наблюдение, обобщение, сравнение, моделирование, эксперимент, анкетирование, интервьюирование.

**Нормативную основу** исследования образуют Конституция Российской  
Федерации, уголовное, уголовно-процессуальное и оперативно-розыскное  
законодательства, иные федеральные законы, подзаконные нормативные акты,  
регулирующие полномочия правоохранительных органов, различных

учреждений, организаций, связанные с предоставлением услуг связи и

возможностью контроля за информацией, передаваемой с помощью средств  
телекоммуникации; нормативную основу составили также отдельные  
положения международного права, затрагивающие проблематику

диссертационного исследования.

**Теоретическая основа исследования** представлена трудами следующих  
авторитетных российских ученых-юристов: Р.Г. Амирова, Н.В. Бахарева,

В.П. Бахина, Р.С. Белкина, В.И. Брылева, А.В. Варданяна, А.Н. Васильева,  
А.И. Винберга, И.А. Возгрина, А.Ф. Волынского, А.Я. Гинзбурга, А.Ю. Головина,  
В.Н. Григорьева, Е.А. Доля, Л.Я. Драпкина, А.В. Дулова, О.А. Зайцева,  
А.А. Закатова, Г.Г. Зуйкова, Е.П. Ищенко, С.Я. Казанцева, Л.М. Карнеевой,  
В.Я. Колдина, А.Н. Колесниченко, В.Е. Коноваловой, С.И. Коновалова,

Н.И. Кулагина, Ю.Г. Корухова, В.П. Лаврова, А.М. Ларина, А.А. Леви,

И.М. Лузгина, П.А. Лупинской, Ю.А. Ляхова, Г.М. Меретукова, В.В. Николюка,  
В.А. Образцова, А.С. Подшибякина, Н.И. Порубова, А.Р. Ратинова,

А.П. Резвана, Е.Р. Россинской, Р.А. Рычкаловой, Э.О. Самитова,

Н.А. Селиванова, Б.П. Смагоринского, А.Б. Соловьева, Л.А. Соя-Серко,

М.С. Строговича, В.Т. Томина, А.Г. Филиппова, А.А. Чувилева, С.А. Шейфера, М.А. Шматова, А.В. Шмонина, С.П. Щерба, П.С. Элькинд, Н.П. Яблокова, И.Н. Якимова, М.Л. Якуб, Н.А. Якубович и других исследователей.

**Эмпирическую базу** исследования составляют следующие источники: - материалы 360 уголовных дел, связанных с хищениями, совершенными с использованием интернет-технологий, расследованных на территории Республики Татарстан, Республики Чувашия, Московской и Ульяновской областей Российской Федерации;

- результаты интервьюирования по предварительно разработанной анкете 265 различных категорий сотрудников правоохранительных органов: следователей (руководителей следственных органов) Следственного комитета РФ и органов внутренних дел, дознавателей органов внутренних дел, оперативных уполномоченных, должностных лиц органов прокуратуры, - по

вопросам, связанным с проблематикой настоящего исследования. Кроме того, эмпирической базой исследования послужила опубликованная следственная и судебная практика, статистические данные, результаты эмпирических обобщений, проведенных другими исследователями.

**Научная новизна** диссертационного исследования заключается в том,  
что автор рассматривает одну из актуальных, недостаточно изученных и  
сложных в теоретическом и практическом отношении проблематику,  
затрагивающую вопросы криминалистического обеспечения расследования  
хищений, совершенных с помощью интернет-технологий. Сформулирована  
авторская научная позиция по вопросу о криминалистической характеристике и  
генезисе хищений, совершенных с помощью интернет-технологий, дается  
критическое переосмысление научных суждений, выраженных иными авторами  
ранее, касающихся проблемных вопросов производства следственных действий  
и оперативно-розыскных мероприятий. Предлагаются авторские рекомендации  
по повышению эффективности данных следственных действий как средств  
формирования доказательственной информации. Впервые в

систематизированном виде представлены рекомендации по предупреждению хищений, совершенных с использованием интернет-технологий.

**Положения, выносимые на защиту**:

1. Выявлены и систематизированы способы подготовки, совершения и сокрытия хищений, совершенных с использованием интернет-технологий, которые автор классифицирует на следующие группы: непосредственный доступ к машинным носителям и информации; дистанционный доступ к машинным носителям и информации; фальсификация входных (выходных) данных и управляющих команд; несанкционированное внесение изменений в существующие программы для компьютерных устройств и создание вредоносных программных средств; незаконное распространение машинных носителей, содержащих компьютерную информацию; комплексные способы.

1. Рекомендованы меры организации взаимодействия следователя и специалистов в области нано-технологий при производстве оперативно-розыскных мероприятий и следственных действий при расследовании хищений, совершенных с использованием интернет-технологий.
2. Способы выявления, фиксации и изъятия материальных следов, указывающих на конкретных лиц, причастных к происшествию; установление обстоятельств, отражающих объективную сторону преступления; время, место и способ его совершения; признаков, указывающих на мотивы и цели совершения преступления.
3. Рекомендации по тактике проведения отдельных следственных действий, таких как осмотр места происшествия, осмотр компьютерных устройств, допрос свидетелей, потерпевших, подозреваемых, назначение и проведение судебных экспертиз. Следственные ситуации, возникающие на различных этапах расследования, задачи и программы действий следователя; проанализирован процесс выдвижения версий, организации и планирования расследования уголовных дел по хищениям, совершенным с использованием интернет-технологий.
4. Меры предупреждения хищений, совершаемых с использованием SMS-сообщений, фальшивых автоматов; организационно-технические меры противодействия, другие меры противодействия, использование одноразовых паролей; рекомендации при сообщении потенциальным преступникам сведений о своей карте, при использовании пластиковой карты для покупок через вебсайты, при работе в сети Интернет и др.
5. Рекомендации по защите компьютерных устройств и программного обеспечения: анализ работы программных средств защиты; контроль их целостности; применение безопасного логина, пароля, антивирусных средств; ограничение физического доступа к программам и оборудованию, предотвращение распространения файловых вирусов; периодическое техническое обеспечение и контроль наличия вирусов; контроль запускаемых

программ, работы компьютерных устройств, сервисное обслуживание специалистами в данном направлении и др.)

**Теоретическая и практическая значимость** результатов исследования  
заключается в том, что, развивая в теоретическом и практическом аспекте одну  
из наиболее сложных юридических проблем, носящих междисциплинарный  
характер, связанных с законодательным ограничением отдельных

фундаментальных гарантий защиты прав личности в результате деятельности  
по расследованию преступлений исследование содержит элементы нового  
знания, направленного на повышение эффективности следственных действий,  
связанных с получением и анализом информации, передаваемой с помощью  
средств телекоммуникации. Результаты настоящего диссертационного

исследования могут найти применение в дальнейших монографических и иных  
научных исследованиях фундаментального и прикладного характера,  
посвященных аналогичной либо смежной тематике. Практические

рекомендации автора, направленные на повышение эффективности

следственных действий, связанных с получением и анализом информации,  
передаваемой с помощью интернет-технологий внедрены в учебный процесс  
кафедры уголовного процесса и криминалистики Казанского государственного  
федерального Университета, кафедры криминалистики Казанского

юридического института МВД России, кафедры криминалистики Восточносибирского института МВД России; кафедры управления органами расследования преступлений Академии управления МВД России, кафедры криминалистики Санкт-петербургского университета МВД России, в практическую деятельность следственного управления, отдела «К» МВД РТ. Отдельные выводы диссертанта могут быть полезны в нормотворческой деятельности по совершенствованию действующего законодательства.

**Апробация результатов исследования**. Диссертация регулярно подвергалась обсуждению на кафедре криминалистики ФГКОУ ВО «Казанский юридический институт МВД России», где она выполнялась. Наиболее важные

положения диссертационного исследования получили освещение в 12 научных статьях автора, в т.ч. в журналах, рекомендованных Высшей аттестационной комиссией РФ для издания результатов диссертационных исследований и 1 учебно-практическом пособии. Диссертант участвовал в научно-практических конференциях всероссийского и международного уровня, проводимых на базе Казанского юридического института МВД России (2001 – 2014 гг.), Казанского федерального университета(2006 – 2014 гг.), а также на семинарах в Московском университете МВД РФ, Дальневосточном юридическом институте МВД РФ (г. 2009 – 2014 гг.), Ростовском юридическом институте МВД России (г. 2009 – 2014 гг.), Академии управления МВД РФ (2014г), Санкт-Петербургском университете МВД РФ(2014г).

**Структура** диссертационного исследования обусловлена поставленными целями и задачами, объектом и предметом исследования. Диссертация содержит введение, 4 главы, объединяющие 15 параграфов, заключение, список используемой литературы, приложения.

## Способы совершения и сокрытия хищений, совершенных с использованием интернет-технологий

Следующей составляющей криминалистической характеристики хищений, совершаемых с применением интернет-технологий, становится личность преступника. Она очень многогранна, обладает своей спецификой и особенностями. Особенностью личности типичных преступников, совершающих хищения с применением интернет-технологий, можно считать высокую степень профессиональной подготовки, умение проводить анализ, систематизировать материал, делать выводы, часто у них имеется хорошее техническое образование. Личность преступника представляет собой основной элемент криминалистической характеристики хищений, осуществляемых при помощи интернет-технологий.

Согласно данным нашего исследования, хищения, совершаемые с применением интернет-технологий, почти осуществляют всегда мужчины, женщины данное преступление совершают только в единичных случаях; у 81% из общего количества задержанных имеется высшее техническое образование. В процессе исследования было установлено, что ряд лиц (приблизительно 13%) получили два высших образования. Данное обстоятельство дает возможность сделать выводы относительно того, что хищения в современном мире с применением интернет-технологий и в области интернет-технологий осуществляют профессионалы, которые вследствие каких-либо причин были недооценены окружающим обществом.

На наш взгляд, наибольшее опасение вызывает то, что российские преступники поддерживают тесные контакты с зарубежными преступниками, проводя с ними регулярный обмен опытом. К примеру, согласно информации МВД России, весной 2013 года сотрудники УБЭП УВД г. Казани обнаружили деятельность хакерской преступной группировки, которая состояла из студентов казанских технических вузов. На протяжении нескольких месяцев они с применением специализированного оборудования, приобретенного в интернете, осуществляли хищения денежных сумм и данных со счетов юридических лиц. Оценка общей суммы причиненного ущерба составила более 2 млн рублей. Распределение ролей в подготовке, совершении и сокрытии хищений, совершаемых с применением интернет-технологий, между участниками преступной группировки было следующим. Первая подгруппа занималась незаконным получением конфиденциальных сведений. Для этого ими была разработана система технических устройств с целью негласного получения данных. Вторая подгруппа согласно полученной информации обрабатывала эти данные, систематизировала их, разрабатывала планы преступной деятельности группы. Третья подгруппа переводила похищенные деньги на счета в офшоры, занималась переводами и распределением данных и денежных средств. Четвертая подгруппа обеспечивала прикрытие остальным группам, уничтожала следы преступлений, разрабатывала алиби, находила и договаривалась с сообщниками.

Пятая подгруппа работала со специалистами по интернет-технологиям в зарубежных государствах, обеспечивая преступную группу необходимыми материалами и орудиями, которые применялись в процессе подготовки и осуществления хищений, совершаемых при применении интернет-технологий.

Анализируя социальный статус лиц, осуществивших хищения при использовании интернет-технологий, нужно принять во внимание, что большинство совершаемых преступлений в статистику не попадает. Наоборот, подробнее всего анализируются как раз те происшествия, которые привлекли повышенное внимание.

Согласно нашим данным, у каждого из лиц, совершивших хищения с применением интернет-технологий, имеются собственные особенности. Так, каждый из них придумывает свой «ник», под которым он известен в компьютерных и глобальных сетях. Происходит перераспределение ролей в различных направлениях преступной деятельности. Такие лица знают исключительно координаты руководителя и имеют возможность с ним общаться. Общение часто происходит с применением определенных каналов для связи. Обычно ни рядовые члены группы, ни заместители руководителя того, с кем общаются, не знают в лицо. Так гарантируется максимальная скрытность, анонимность и безопасность лидера. Подобная ситуация стала возможна благодаря мобильным средствам функционирующих сегодня систем цифровой электросвязи: сотовая радиотелефонная и спутниковая связь, компьютерная сеть Интернет.

В абсолютном большинстве случаев (97%) преступники, совершавшие хищения с применением интернет-технологий, были служащими государственных организаций или учреждений, применяющих компьютерные технологии в собственных производственных процессах, при этом 30% из них непосредственно имели отношение к использованию компьютерной техники. С точки зрения исследователя, интересным является то, что на каждую тысячу хищений, совершаемых с применением интернет-технологий, лишь 7 осуществляются программистами-профессионалами.

В соответствии с данными нашего исследования, преступник из числа работников организации – образцовый служащий, который получил соответствующее образование. Обычно указанные лица никаких преступлений раньше не совершали. Часто они являются руководителями различного уровня, обладают определенными распорядительными функциями, однако не отвечают непосредственно за конкретные участки. К моменту осуществления хищений при помощи интернет-технологий преступники по уровню образования имели: 40% – высшее; 40% – среднее специальное; 20% – среднее.

Наиболее часто хищения при использовании интернет-технологий осуществляются преступными группами с устойчивым составом, которым характерна мобильность, серьезная техническая оснащенность, четкое разделение функций, ярко очерченная корыстная мотивация, прекрасно продуманная система по сокрытию следов совершенных преступных деяний. Самая большая опасность и проблематичность для определения и раскрытия исходит от преступных группировок, которые имеют в составе высококвалифицированных профессионалов, имеющих специальные знания в сфере негласного получения, а также защиты компьютерной информации. Большей частью хищения с применением интернет-технологий, произведенные вышеуказанными субъектами, остаются латентными.

## Особенности первоначального этапа расследования хищений, совершенных с использованием интернет-технологий

Необходимо остановиться на ошибках. Например, следователь думает, что информация и вещественные доказательства имеются у него в достаточном количестве, может отнестись формально к проведению необходимых следственных действий по их закреплению, обычно ограничиваясь допросами заинтересованных лиц. В основном трудности в доказывании вины конкретных лиц связаны с тем, что лицом, проводящим расследование, может быть упущена на первоначальном этапе расследования детализация обстоятельств по главным пунктам обвинения.

Третья ситуация характеризуется тем, что обвиняемый полностью отрицает факты совершения хищений, совершенных с использованием интернет-технологий (6% случаев). Третья ситуация характеризуется тем, что обвиняемый отказывается от дачи показаний.

Задачи: преодолеть отказ о дачи ложных показаний; определить направления поиска дополнительных следственных мероприятий; оценить имеющиеся по делу доказательства; поиск дополнительных доказательств, подтверждающих факт пребывания подозреваемого и потерпевшего на месте происшествия в определенное время; получить новые данные, подтверждающие системный характер действий подозреваемого; выявить новые следы, свидетельствующие о совершении хищений, совершенных с использованием интернет-технологий.

Следователю необходимо выполнять следующие действия: планируя дополнительный допрос обвиняемого, следователь (дознаватель) учитывает такие его элементы, как организационный, содержательный и тактический (место, время, количество участников, наличие технических средств, определение обстоятельств, подлежащих выяснению, использование тактических приемов допроса, направленных, в частности, на установление психологического контакта с допрашиваемым, и т.д.); дополнительные, повторные допросы потерпевших, свидетелей, знакомых обвиняемого; предъявление для опознания предметов; очная ставка; следственный эксперимент; проверка показаний на месте; назначение дополнительных экспертиз (компьютерно-технической и судебно-бухгалтерской экспертизы, судебно-медицинских; криминалистических; комплексной медико криминалистической и т.д.); наведение справок, наблюдение, снятие информации с технических каналов связи, прочесывание местности.

В четвертой ситуации обвиняемый признает свою вину частично (9,1% случаев). Он считает, что доказательства, выдвинутые следствием (дознанием), необоснованные. Поэтому заинтересованность обвиняемого в сокрытии перед следствием (дознанием) фактов своей преступной деятельности очевидна.

В данной ситуации следователю (дознавателю) необходимо скон центрировать внимание на следующих задачах: преодолеть попытку дачи ложных показаний; подготовиться к противоречивому и негативному поведению данных лиц во время проведения допроса; определить направления поиска дополнительных следственных действий; оценить имеющиеся по делу доказательства; поиск дополнительных доказательств, подтверждающих факт пребывания подозреваемого и потерпевшего на месте происшествия в определенное время; получить новые данные, подтверждающие системный характер действий подозреваемого; выявить новые следы, свидетельствующие о совершении хищений с использованием интернет-технологий.

Следователю необходимо выполнять следующие действия: допрос обвиняемого; дополнительные, повторные допросы потерпевших и свидетелей; предъявление для опознания; очная ставка обвиняемого с потерпевшим, свидетелями; выявление новых свидетелей, следственный эксперимент, проверка показаний на месте; назначение судебно психологической, судебно-психиатрической экспертизы обвиняемого; предъявление для опознания предметов; очная ставка; следственный эксперимент; проверка показаний на месте; назначение дополнительных экспертиз (компьютерно-технической и судебно-бухгалтерской экспертизы, судебно-медицинских; криминалистических; и т.д.); наведение справок, наблюдение, снятие информации с технических каналов связи, прочесывание местности.

В пятой ситуации преступник признается в хищениях, совершенных с использованием интернет-технологий, но не признается в других преступлениях (вымогательстве и других составляющих 2% случаев).

В данной ситуации следователю (дознавателю) необходимо скон центрировать внимание на следующих задачах: преодолеть попытку дачи ложных показаний; подготовиться к преодолению негативного поведения данных лиц во время проведения допроса; определить направления поиска дополнительных следственных мероприятий; оценить имеющиеся по делу доказательства; поиск дополнительных доказательств, подтверждающих факт пребывания подозреваемого и потерпевшего на месте происшествия в определенное время; получить новые данные, подтверждающие системный характер действий подозреваемого; выявить новые следы, свидетельствующие о совершении хищений, совершенных с использованием интернет-технологий.

Алгоритм действий следователя: повторный углубленный допрос свидетелей (т.к. ранее неизвестные эпизоды других преступлений, так и дополнительных хищений становятся известны с их слов); выявление дополнительных свидетелей; допрос обвиняемого, допрос свидетелей, установленных спустя определенный промежуток времени после совершения преступления; повторный допрос свидетелей, допрошенных на первоначальном этапе расследования хищений; проведение очных ставок, следственный эксперимент, проверка показаний на месте; назначение дополнительных судебно-медицинских экспертиз; предъявление для опознания предметов; очная ставка; следственный эксперимент; проверка показаний на месте; назначение дополнительных экспертиз (компьютерно-технической и судебно-бухгалтерской экспертизы, судебно-медицинских; криминалистических; комплексной медико-криминалистической и т.д.); наведение справок, наблюдение, снятие информации с технических каналов связи.

Анализ уголовных дел по хищениям, совершенным с использованием интернет-технологий, относящихся к указанной ситуации, свидетельствует, что поведение преступника в момент его допроса может развиваться по трем направлениям: во-первых, обвиняемый, отрицая вину, сам излагает картину произошедшего события в 55,6 % случаев; во-вторых, в своих показаниях преступник ссылается на алиби (находился в ином месте) в 22,4% случаев; в-третьих, молчит, полностью отказываясь от дачи показаний, в 22% случаев. Работа следователя (дознавателя) должна быть направлена на тщательный анализ собранных по делу доказательств. Затем на выявление свидетелей, характеризующих личность обвиняемого; установление сотрудников (коллег), которые могли бы дать показания по факту обращения потерпевшего за помощью.

## Осмотр машинного документа в ходе расследования хищений, совершенных с использованием интернет – технологий

Находясь уже на месте проведения обыска, рекомендуется вести себя таким образом: - внезапно и быстро зайти в объект, в котором планируется обыск (либо в несколько помещений одновременно); - в случае оказания сопротивления лицами, находящимися на объекте, - обыскиваемого, родственников, сотрудников организации, охранников (сторожей) и т. д. - срочно принять меры для нейтрализации сопротивления и быстрейшему проникновению в помещение для обыска; - место обыска должно быть под надежной охраной и наблюдением; охраняться должны обыскиваемые площади по всему периметру, компьютерно-технические средства обеспечения данными, хранилища МНИ, пульты (пункты) связи, электропитания и охраны, которые находятся на обыскиваемом объекте (на производственной площади, в помещении, здании), средства защиты от незаконного доступа, хранилища ключей регламентного и аварийного доступа к компьютерно-техническим средствам по обеспечению информацией, помещениям, прочим объектам (пункты, пульты, сейфы, стенды и т. д.).

Следователь должен иметь в виду, что к уничтожению или изменению машинных данных, их носителей и/или компьютерно-технического средства обеспечения данными, которые в будущем могут выступить доказательствами по делу, ведут как манипуляции с компьютерно-техническими средствами обеспечения информацией, так и выключение или включение их электропитания. В связи с этим электротехническое оборудование, а также инструменты электротехнических систем, которые имеются на обыскиваемом объекте, должны присутствовать до факта их осмотра в том положении в пространстве и техническом состоянии, которое было на начало обыска. Поэтому нужно соблюдать определенные условия: - не позволять никому из присутствующих на обыскиваемом объекте лиц (кроме приглашенных специалистов) касаться компьютерно технических средств по обеспечению данными и к источникам питания электрического оборудования, независимо от причины, даже если обыскиваемый добровольно согласился выдать искомую информацию, документ либо предмет; - не позволять никому включать-выключать электроснабжение объекта, не спросив разрешения специалиста; - если к моменту начала обыска выключено электроснабжение объекта, тогда до его включения нужно отключить из электросети все компьютерно-технические средства по обеспечению информацией, зафиксировав предварительно в протоколе порядок подключения их к электропитанию, тактико-технические параметры, расположение и порядок отключения компьютерно-технических средств по обеспечению информацией от них; - нельзя проводить самостоятельно никаких манипуляций с электрооборудованием, а также с компьютерно-техническими средствами обеспечения информацией, в случае когда их результат заранее неизвестен; - если обыскиваемый или другие лица, находящиеся в месте обыска, настойчиво пытаются проникнуть к компьютерно-техническим средствам обеспечения данными, пунктам управления, связи и энергоснабжения, а также к прочему оборудованию и техническим средствам, нужно принимать меры по перемещению таких лиц в иное помещение (которое не подлежит обыску) и обязательно фиксировать данное событие в протоколе. Затем, по нашему мнению, нужно:

1. Установить и выключить специальные средства по защите информации и компьютеров от незаконного доступа, в особенности те, что автоматически стирают данные и МНИ, в случае нарушения процедур доступа к компьютерно-техническим средствам обеспечения данными и машинной информации, режима использования их и/или правил, установленных для работы с ними; установить ключ, пароль дешифрования-шифрования данных и санкционированного доступа.

2. Определить наличие телекоммуникационных связей между компьютерно-техническими средствами обеспечения данными с каналами электросвязи по моделям «персональный компьютер – персональный компьютер», «персональный компьютер - сервер», «персональный компьютер - периферийное устройство», «персональный компьютер средство электросвязи», «периферийное устройство - периферийное устройство», «персональный компьютер - канал электросвязи», «периферийное устройство - средство (канал) электросвязи», а также наоборот. Если в наличии имеется компьютерная сеть любого уровня конфигурации, тогда сначала осмотру и обыску должен быть подвергнут управляющий центральный компьютер (компьютер процессингового центра, сервер, узел охранной системы, связи и т. д.). Такое компьютерно техническое средство обеспечения данными хранит в постоянной и оперативной памяти самую большую часть машинных данных, управляет остальными компьютерно-техническими средствами обеспечения данными, имеет обратную и прямую связь с ними и, чаще всего, обладает программой для установления автоматической связи между собой всех компьютеров, объединенных в одну сеть (что-то вроде «электронного журнала» для учета всех параметров работы подключенных в сеть компьютерно-технических средств для обеспечения данных - их абонентские, позывные, индивидуальные номера и т. д., даты с указанием точного времени по каждому соединению в ходе обмена данными, вид сеанса связи и его длительность, характеристики получаемых и передаваемых данных, аварийные и нештатные ситуации, различные сбои при работе некоторых компьютерно-технических средств для обеспечения данными (периферийного оборудования, рабочих станций), пароли операторов и идентификационные коды, попытки нештатного или несанкционированного доступа и другое).

## Общие и специальные меры профилактики хищений, совершенных с использованием интернет-технологий

Утверждение эффективных мероприятий по борьбе с нарушителями правил защиты СКТ. Как было выявлено на практике, самым надежным способом повышения эффективности мероприятий по охране компьютерно технических средств можно назвать обучение и ознакомление компетентных сотрудников с используемыми в определенной компании организационно техническими мерами обеспечения безопасности.

Помимо этого, обязательно должны быть внедрены следующие организационные меры: 1) Всем лицам, которые имеют санкционированный доступ к компьютерно-техническим средствам обеспечения информацией, необходимо определить категории допуска, то есть нужно выявить сферу рабочих интересов каждого из сотрудников, типы информации, которые им доступны, и тип разрешения данного доступа, который определяется полномочиями лица на осуществление определенных манипуляций с СКТ согласно его непосредственным функциональным обязанностям. 2) Необходимо определить административную ответственность для лиц за сбережение и правомерность доступа к информационным ресурсам, которые есть в наличии у организации. При этом ответственность должна быть назначена за каждый их вид на конкретное лицо. 3) Нужно наладить периодическую систему контроля над эффективностью защиты компьютерной информации методом реализации регламентных работ лицом, несущим ответственность за безопасность и компетентных экспертов (специалистов), привлеченных из других организаций. 4) Следует классифицировать информацию, исходя из ее важности, и дифференцировать на основании этого защитные меры, а также определить порядок ее охраны и ликвидации. 5) Необходимо организовать физическую защиту компьютерных систем, в которых хранится ценная информация (физическая охрана). Мы считаем, что, помимо внедрения организационно-управленческих мер, значительную профилактическую роль в профилактике хищений с применением интернет-технологий может играть комплекс мероприятий технического характера. К нему относятся технические способы обеспечения безопасности средств компьютерной техники, к примеру: защита от несанкционированного доступа, от стихийных бедствий и технических проблем работы, таких как пожары, отключение электричества, потопы и прочее, от хищений средств компьютерной техники, саботажа, взрывов (диверсий), резервирование самых важных средств компьютерной техники, грамотная организация коммуникационных ресурсов и сетей, внедрение охранно-пожарной сигнализационной системы и прочих рубежей охраны.

По нашему мнению, формально их можно разделить на 3 основные подгруппы, в зависимости от специфики и характера охраняемого объекта: Аппаратные методы применяются для обеспечения защиты аппаратных устройств и компьютерной техники от неблагоприятных физических воздействий со стоны злоумышленников и для перекрытия потенциальных каналов утечки секретной информации и данных, которые образуются за счет неблагоприятного воздействия электромагнитных излучений и наводок, акустиковибрационных сигналов и прочих факторов, которые мы рассматривали предыдущих главах.

Реализация этих методов на практике, как правило, осуществляется путем применения разных технических средств особого назначения.

К примеру, обеспечение защиты информации на уровне управляющих команд заключается в: защите информации в случае ее передачи по разным связным каналам между пользователем и компьютерно-технической системой либо между разными устройствами; обеспечении прав доступа исключительно к разрешенной информации, хранящейся в компьютерных системах, и совершение с ней только правомерных операций. При передаче информации для обеспечения защиты обычно применяются различные способы ее шифрования перед тем, как ввести ее в связной канал или на физический носитель с возможностью последующей расшифровки. На практике было выявлено, что различные способы шифрования данных позволяют надежно укрыть смысл сообщения. К примеру, в США, согласно директиве Министерства финансов, в 1984 году каждая общественная и частная организация должна была установить процедуру шифрования секретных коммерческих данных по системе DES, которую Национальное бюро стандартов официально утвердило с 1978 года.

Иной подход, предполагающий построение системы защиты к праву доступа, основывается на контроле информационных течений и разделении объектов и субъектов доступа на категории секретности (классы и степень допуска, которые учитывают полномочия пользователей и содержание информации). 1

Перечисленные нами способы контроля позволяют использовать поток информации для чтения, если степень информационного объекта-источника отвечает или не является выше категории субъекта-получателя данных, а для записи, если уровень субъекта-источника отвечает либо превышает степень секретности информационного объекта.2