АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЮРИДИЧЕСКИЙ ИНСТИТУТ АГУ

приоритет2030^
лидерами становятся

В.В. Поляков

Основы методики расследования компьютерных преступлений

Министерство науки и высшего образования Российской Федерации
Алтайский государственный университет

В.В. Поляков

ОСНОВЫ МЕТОДИКИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Учебное пособие

Барнаул
Издательство
Алтайского государственного
университета
2024

УДК 343.97:343.23:004(075.8)
ББК 67.523я73+67
П 542

Рецензент:
О.В. Беспечный, кандидат юридических наук, доцент

Поляков, Виталий Викторович.
П 542 **Основы методики расследования компьютерных преступлений** : учебное пособие / В.В. Поляков ; Министерство науки и высшего образования РФ, Алтайский государственный университет. — Барнаул : Изд-во Алт. ун-та, 2024. — 121 с.

ISBN 978-5-7904-2863-0.

В пособии рассмотрены теоретические основы криминалистической методики расследования компьютерных преступлений. Приведены базовые положения, относящиеся к содержанию криминалистической характеристики этих преступлений и их расследованию. Описаны теоретические представления о криминалистическом предупреждении компьютерных преступлений. Представлены методические материалы, указания, рекомендации и задания для проведения семинарских занятий по учебным дисциплинам, ориентированным на получение криминалистических знаний по расследованию компьютерных преступлений. Пособие предназначено для преподавателей юридических дисциплин, студентов, обучающихся по юридическим направлениям подготовки ВУЗов, а также специалистов и сотрудников правоохранительных органов. Представленные методические материалы могут быть также использованы при повышении квалификации и переподготовке специалистов юридического профиля.

УДК 343.97:343.23:004(075.8)
ББК 67.523я73+67

Учебное пособие издано при финансовой поддержке средствами программы развития ФГБОУ ВО «Алтайский государственный университет» по проекту «Энциклопедия противодействия киберпреступности» программы «Приоритет - 2030».

ISBN 978-5-7904-2863-0

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день серьезной является проблема качественного и количественного роста компьютерных преступлений. Усугубляется данная проблема тем, что раскрываемость компьютерных преступлений уже не одно десятилетие остается на низком уровне, причем, с развитием информационных технологий и появлением высокотехнологичных преступлений сложности в выявлении и расследовании данных преступлений только увеличивается. По этой проблеме Генеральный прокурор РФ высказался, что «правоохранительные органы демонстрируют низкую способность противостоять новому виду преступности»[1]. От государства требуется скорейшее принятие мер для обеспечения защиты граждан от таких преступных посягательств.

В определенной степени сложившаяся ситуация связана с необходимостью улучшения образования в области учебных дисциплин криминалистического цикла, нацеленных на противодействию компьютерным преступлениям. Существующие криминалистические материалы по противодействию киберпреступности зачастую носят либо слишком общий, либо слишком частный характер, не системны, оторваны от нужд практики, не адекватны современным способам совершения преступлений. Остро требуются современные учебные материалы, направленные на рассмотрение вопросов о признаках и особенностях компьютерных преступлений, способах их совершения, механизме следообразования электронно-цифровых следов, обстановке преступлений, средств совершения таких преступлений, личностных особенностей преступников и потерпевших, причин и условий, способствующих совершению таких преступлений. Необходимо решение вопросов

[1] Выступление Генерального Прокурора РФ Краснова И.В. на заседании коллегии Генеральной прокуратуры РФ 17 марта 2020 года // URL: http://www.kremlin.ru/events/president/news/62998

прикладного криминалистического характера, относящихся к формулированию современных подходов по выявлению электронно-цифровых следов и их изъятию, фиксации, хранению, исследованию и оценке, организации расследования и тактики производства следственных действий, недопущения распространенных следственных ошибок и упущений, преодоления противодействия расследованию, разрешения криминалистических ситуаций на всех этапах криминалистической деятельности, возможностей применения мер криминалистического предупреждения компьютерных преступлений.

В условиях цифровизации общества необходимо получение новых и совершенствование имеющихся компетенций, формируемых из знания о современных угрозах со стороны киберпреступности, а также теории и практики расследования и предупреждение таких преступлений. Необходимым фактором эффективного современного обучения является практико-ориентированный комплексный подход, заключающийся в совершенствовании имеющихся и получении новых компетенций в области правильной оценки современных угроз со стороны киберпреступности, знания теории и практики расследования и предупреждения таких преступлений, а также развития практико-ориентированных умений и навыков эффективного им противодействия в различных криминалистических ситуациях.

Настоящее учебное пособие направлено на совершенствование образовательных методик противодействия компьютерным преступлениям с учетом современных научно-педагогических стандартов криминалистической науки. Данные материалы могут быть использованы слушателями курсов повышения квалификации по юридическим направлениям подготовки. При этом настоящее пособие предполагает повышение юридической и технической квалификации, прежде всего, сотрудников правоохранительных органов, участвующих в выявлении и расследовании компьютерных преступлений.

Структура учебного пособия состоит из введения, трех глав, заключения и списка рекомендуемой литературы. Разделы объединены единой логической последовательностью изложения материала по циклу специальных дисциплин в области расследования и предупреждения компьютерных преступлений. В первой главе содержится система учебно-методических материалов для проведения семинарских занятий по дисциплине «Криминалистическая характеристика компьютерных преступлений», обеспечивающей базовые знания о признаках и особенностях данного общественно опасного явления. Во второй главе содержатся материалы по дисциплине «Особенности расследования компьютерных преступлений», посвященной изучению криминалистических тактико-технических и методических возможностей расследования данных преступлений. В третьей главе раскрываются основы дисциплины «Предупреждение компьютерных преступлений», содержащей дополнительные представления о понимании закономерностей, способствующих совершению компьютерных преступлений, сложностях их расследования и возможностях по принятию конкретных мер по устранению этих обстоятельств и пресечению негативных последствий от таких преступлений.

Каждая глава пособия содержит также учебные материалы, необходимые для проведения семинарских занятий. Приведены примерные планы этих занятий, перечни вопросов для самоконтроля и контроля полученных знаний, представлены темы для подготовки учащимися рефератов и научных докладов, по каждой из тем приводится рекомендуемая литература.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

1.1. Теоретические положения криминалистической характеристики компьютерных преступлений

Криминалистическая характеристика преступлений отражает закономерности способов и следообразования преступной деятельности субъекта по приготовлению, совершению и сокрытию преступлений в различных криминальных ситуациях. Формирование теоретических моделей элементов криминалистической характеристики компьютерных преступлений происходит путем обобщения судебно-следственной практики и иных источников информации, например, экспертных мнений, использования данных иных преступлений, если они близки к предметной области исследования. Ценность криминалистической характеристики повышается при ее адаптации к специфике отдельных регионов государства.

В теории криминалистики нет единого определения криминалистической характеристики преступлений. В наиболее краткой формулировке под ней можно понимать «наиболее существенные признаки, отличительные свойства по совершению отдельных видов и групп преступлений»[2]. С точки зрения А. Г. Филиппова она представляет собой «систему присущих тому или иному виду преступлений особенностей, имеющих наибольшее значение для расследования и обусловливающих применение криминалистических методов, приемов и средств»[3]. По мнению Р. С. Белкина в криминалистическую характеристику преступлений следует включать «характеристику исходной информации, систему данных о способе

[2] Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений: монография. Томск: Изд-во Томского ун-та, 1985. С. 162.

[3] Филиппов А. Г. Общие положения методики расследования отдельных видов и групп преступлений (криминалистической методики): Учеб. 2-е изд. М., 2000. С. 407.

совершения и сокрытия преступления и типичных последствиях его применения, личности вероятного преступника и вероятных мотивах и целях преступления, личности вероятной жертвы преступления, о некоторых обстоятельствах совершения преступления (место, время, обстановка)»[4]. А.А. Бессонов определяет криминалистическую характеристику преступлений как научную категорию, представляющую собой информационную модель, отражающую криминалистическую сущность преступлений определенного вида (подвида, криминалистически схожих групп), заключающуюся в сведениях об имманентных им криминалистически значимым признакам и их закономерным связям между собой[5]. Во многих криминалистических исследованиях криминалистическая характеристика преступлений рассматривается как теоретическая модель[6]. Так, например, А.С. Князьков, отмечает, что «главное предназначение» криминалистической характеристики заключается в том, чтобы выступать в качестве модели определенной группы преступлений[7].

Конкретный перечень элементов криминалистической характеристики преступлений в криминалистической науке является дискуссионным. В любом случае, в качестве криминалистически значимой информации должна выступать та, которая отражается от структурообразующих элементов преступления: субъекта преступления, мотива и цели его деяния; ситуации преступления; причин и условий, способствовавших совершению преступления; способа, места и времени преступления; предмета посягательства; связи между субъектами преступления и обстановкой

---

[4] Белкин Р. С. Курс криминалистики. М., 1997. Т. 3. С. 315-316.

[5] Бессонов А.А. Частная теория криминалистической характеристики преступлений // автореферат диссертации на соискание ученой степени доктора юридических наук / Акад. упр. МВД РФ. Москва, 2017. С. 11.

[6] Россинская Е.Р., Семикаленова А.И. Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере "кибершантажа") // Вестник Томского государственного университета. Право. 2021. № 42. С. 69.

[7] Князьков А.С. Криминалистика: курс лекций / Под ред. проф. Н.Т. Ведерникова. Томск: Изд-во «ТМЛ-Пресс», 2008. С. 905.

совершения преступления, соучастниками, свидетелями, потерпевшими; наступившими последствиями преступного посягательства; следов-последствий преступлений и других источников информации[8].

Для различных видов и групп преступлений существует свой набор элементов криминалистической характеристики преступлений, который может отличаться не только по их значимости, но и по количеству. Специфика компьютерных преступлений находит свое отражение, например, в таком важном элементе криминалистической характеристики как средства совершения преступлений, без которых не может состояться ни одно криминальное деяние, в то время как во множестве традиционных преступлений общеуголовной направленности данный элемент может отсутствовать, как например при изнасиловании.

Криминалистические характеристики преступлений могут отличаться в зависимости от критерия классифицирования, например, в зависимости от уровня обобщения в криминалистике выделяются родовые, групповые, видовые, межвидовые, базовые, усеченные, сквозные и многие иные виды криминалистических характеристик преступлений[9]. При этом, чем уже уровень обобщения преступлений, тем конкретнее по ним данные и выше практикоориентированность такой характеристики в методике расследования. Это важно, поскольку основная роль криминалистической характеристики преступлений выражается в ее прикладном назначении. Выделенные в теоретических целях элементы криминалистической характеристики преступлений находятся в неразрывной связи друг с другом и отсюда имеют причинно-следственные (строгие) и корреляционные (не строгие)

[8] Криминалистика: учебник / под ред. Л.Я. Драпкина, В.Н. Карагодина. – М.: Юрид. лит., 2004. – С. 456.

[9] Бессонов А.А. Криминалистическая характеристика преступлений в цифровую эпоху // Развитие научных идей профессора Р.С. Белкина в условиях современных вызовов (к 100-летию со дня рождения) : сборник научных статей по материалам Международной научно-практической конференции «63-и криминалистические чтения» (Москва, 20 мая 2022 г.) : в 2 ч. / редкол. : Ю.В. Гаврилин, Б.Я. Гаврилов, С.Б. Россинский, Ю.В. Шпагина. – М.: Академия управления МВД России, 2022. Ч. 1. С. 54-62.

зависимости. Знания таких зависимостей особенно полезны на первоначальном этапе расследования преступлений, когда у следствия имеется минимум сведений о преступлении и количество криминалистических версий наиболее велико. В таких условиях, основываясь на теорию криминалистической характеристики, следователь, получая информацию о любом элементе преступления, с ее помощью может выстроить цепочку предположений об иных элементах, находящихся во взаимосвязи. Так, например, получив сведения о доступе к компьютерной информации, осуществленном по локальной сети, можно сузить круг подозреваемых до тех лиц, которые имели выход в эту сеть. За счет знания корреляционных зависимостей существенно экономятся время и силы по установлению обстоятельств, входящих в предмет доказывания, выдвигаются и проверяются более вероятные криминалистические версии, осуществляется эффективное планирование расследования, реализуются правильные организационно-тактические решения, сокращается количество упущений и ошибок расследования.

С помощью криминалистической характеристики преступлений оказывается непосредственное влияние на построение оптимальной криминалистической методики предварительного, а затем и судебного следствия. Своевременное обобщение данных о типичном и особенном по заданной общности преступлений чрезвычайно важно для криминалистики не только в целях расследования преступлений, но и для выработки адекватных мер криминалистического предупреждения преступлений.

Таким образом, криминалистическая характеристика преступлений — это научная абстракция, в которой находит отражение в обобщенном виде совокупность взаимосвязанных, криминалистически значимых данных о преступлениях определенного вида или группы, знание которых позволяет методически правильно организовать расследование[10].

[10] Поляков В.В. Особенности расследования неправомерного удаленного доступа к

Особенности компьютерных преступлений часто проявляются в технически сложных способах их совершения и оставляемой при этом специфической следовой картине, включающей особый вид следов - электронно-цифровых. Обстановка совершения таких преступлений также весьма необычна, поскольку объективная сторона преступной деятельности разворачивается в кибернетическом пространстве.

Далее приводимые учебно-методические материалы содержат указания, рекомендации и иную информацию по проведению занятий по учебной дисциплине «Криминалистическая характеристика компьютерных преступлений». Даны примерные планы семинарских занятий и примерный перечень вопросов для самоконтроля и зачета, представлены темы для подготовки учащимися рефератов и научных докладов, по каждой из тем приведена необходимая для подготовки литература.

Темы семинарских занятий отражают последовательность изучения курса и позволяют наиболее полно изучить учебный материал. Настоящие учебно-методические материалы рекомендуется использовать вначале обучения по циклу дисциплин, направленных на противодействие компьютерным преступлениям, поскольку их содержание охватывает вопросы криминалистического описания признаков и особенностей преступной деятельности, без понимания которых невозможно расследовать такие специфические преступления.

К каждой теме практического занятия приводятся контрольные вопросы и подробный список дополнительной литературы, которая рекомендуется для изучения. Выбор литературы к теме семинарского занятия определяется необходимостью более глубокого изучения отдельных вопросов темы, обращения к различным научным взглядам. В некоторых темах курса следует изучить материалы судебной практики расследования компьютерных преступлений, необходимые для получения аналитических выводов и

компьютерной информации : дис. ... канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 247 с.

обобщения правоприменительной практики, что должно позволить выявлять и конкретизировать информацию, относящуюся к элементам криминалистической характеристики компьютерных преступлений.

При изучении курса «Криминалистическая характеристика компьютерных преступлений» предполагается зачет как форма итогового контроля. В качестве промежуточного контроля предусмотрено выполнение индивидуальных научно-практических заданий и тестирование.

1.2. ТЕМА 1. ПОНЯТИЙНЫЙ АППАРАТ В СФЕРЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Контрольные вопросы к занятию:

1. Основные понятия информационной безопасности и компьютерных преступлений.
2. Компьютерной информация, охраняемая уголовным законом.
3. Понятие компьютерные преступления. Соотношение с категориями преступления в сфере компьютерной информации, киберпреступления, информационные преступления, высокотехнологичные преступления.
4. Проблемы ведения новых терминов и определений: электронные доказательства электронный документ; электронно-цифровые (виртуальные) следы; удаленный (дистанционный) доступ к компьютерной информации; высокотехнологичные способы совершения компьютерных преступлений, транснациональные (трансграничные преступления), кибтерроризм и киберэкстремизм.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Вехов В. Б. Понятие и механизм образования электронно-цифровых следов // Использование современных информационных технологий и проблемы информационной безопасности в деятельности правоохранительных органов: Межвузовский тематический сборник научных трудов. - Калининград: Изд-во Калинингр. ЮИ МВД России, 2009. - С. 62-72.
2. Зверянская, Л.П. Современные проблемы исследования криминалистических особенностей киберпреступлений / Л.П. Зверянская // Приоритетные научные направления: от теории к практике. – 2015.- № 15.- С.127-132.

3. Князьков, А.С. Криминалистическая характеристика преступления в контексте его способа и механизма / А.С. Князьков // Вестник томского государственного университета.- 2011. - №1.- С.51.64.

4. Поляков В.В. К вопросу о противодействии высокотехнологичной транснациональной преступности / В.В. Поляков // Актуальные проблемы отечественной криминалистики: современные тенденции : сборник материалов Международной научно-практической конференции, посвященной памяти Заслуженного юриста РФ, Заслуженного деятеля науки РФ, Заслуженного профессора Московского университета, доктора юридических наук, профессора Николая Павловича Яблокова. - М.: МГУ имени М.В. Ломоносова. Юридический факультет, 2023. – С. 367-374.

5. Поляков В.В. Понятие «высокотехнологичные преступления» в криминалистике // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. 2023. – Т. 28. – № 4. – С. 151 - 188.

6. Поляков, В.В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике / В.В. Поляков, А.В. Шебалин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : матер. одиннадцатой Междунар. науч.-практ. конф. в 2-х частях. – Барнаул : Барнаульский юридический институт МВД России, 2013. – Ч. 1. – С. 123-125.

7. Поляков, В.В. Об использовании новых понятий при доказывании преступлений в сфере компьютерной информации / В.В. Поляков // Российская юридическая наука : состояние, проблемы, перспективы : матер. Всеросс. науч.-практ. конф., посвященной 45-летию юридического образования на Алтае, 19-20 сентября 2008. – Барнаул : Изд-во АлтГУ, 2008. – С 427 - 431.

8. Хижняк Д.С. Методологические основы расследования транснациональных преступлений: модельный подход: автореф. дис. д-ра. юрид. наук. - М., 2018.

9. Шурухнов, Н.Г. Современная преступность (истоки, направленность, техническая оснащенность, способы совершения, сокрытия): содержание рекомендаций по раскрытию и расследованию / Н.Г. Шурухнов // Известия Тульского государственного университета. Экономические и юридические науки. - 2013.- № 4-2. - С. 123-136.

1.3. ТЕМА 2. ПРАВОВЫЕ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Понятие и содержание уголовно-правовой и криминологической характеристики компьютерных преступлений.
2. Понятие и содержание криминалистической и оперативно-розыскной характеристики компьютерных преступлений.
3. Соотношение данных характеристик.
4. Источники и принципы построения криминалистической характеристики компьютерных преступлений.
5. Проблемы выделения элементов криминалистической характеристики компьютерных преступлений. Корреляционные взаимосвязи элементов криминалистической характеристики компьютерных преступлений

На проведение занятия отводится 4 часа.

Дополнительная литература

1. Азиян, В.Г. Исследование проблемы разработки криминалистической характеристики компьютерных преступлений В.Г. Азизян, Н.И. Журавленко // Евразийский юридический журнал. - 2014. - № 6 (73) - С. 183-187.
2. Афанасьева, И.В. Выявление латентной преступности в России и зарубежных странах / И.В. Афанасьева, Ю.С. Афонина // Актуальные вопросы борьбы с преступлениями.- 2015. - № 2. - С. 46-49.
3. Бессонов А. А. Объект (предмет) преступного посягательства как элемент криминалистической характеристики преступлений / А. А. Бессонов // Вестник Калмыцкого института гуманитарных исследований РАН. – 2014. - № 4. - С. 231.

4. Гавло, В.К. Криминалистическая характеристика неправомерного доступа к компьютерной информации / В.К. Гавло, В.В. Поляков // Труды Сибирского института знаниеведения / под ред. Е.В. Ушаковой, Ю.В. Колюжова – Барнаул – Москва : Изд-во Алт. ун-та, 2007. – Вып. 4. – С. 96 - 100.

5. Гавло, В.К. Криминалистическая характеристика преступлений в сфере компьютерной информации / В.К. Гавло, В.В. Поляков // Право и государство : приоритеты XXI века : матер. Всерос. науч.-практ. конф. / под ред. В.Я. Музюкина, Е.С. Аничкина. – Барнаул : Изд-во Алт. ун-та, 2007. – С. 503 - 507.

6. Гавло, В.К. Некоторые аспекты разработки криминалистической характеристики / В.К. Гавло, В.В. Поляков // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники: проблемы, тенденции, перспективы : матер. Всерос. конф. - М.: МАКС Пресс, 2005. – С. 14-18.

7. Гармаев Ю. П. Теоретические основы формирования криминалистических методик расследования преступлений: монография. - Иркутск: ИЮИ ГП РФ, 2003. - 342 с.

8. Зверянская, Л.П. Современные проблемы исследования криминалистических особенностей киберпреступлений / Л.П. Зверянская // Приоритетные научные направления: от теории к практике. – 2015.- № 15.- С.127-132.

9. Кардашевская М. В. Источники развития криминалистической методики как раздела криминалистики; связь с другими отраслями научного знания // Вестник Московского университета МВД России. - 2015. - № 2. - С. 127-129.

10. Князьков, А.С. Криминалистическая характеристика преступления в контексте его способа и механизма / А.С. Князьков // Вестник томского государственного университета.- 2011. - №1.- С.51.64.

11. Корнеев, И.Г. Криминалистическая характеристика компьютерных преступлений / И.Г. Корнеев // Алгоритмы, методы и системы обработки данных. - 2007. - № 12. - С. 99-103.

12. Кушниренко, С.П. О понятии преступлений, совершаемых в сфере высоких технологий (криминалистический аспект) / С.П. Кушниренко // Криминалистъ.- 2008. -№ 1. -С. 27-29.

13. Мнацаканян, А.В. Преступления в сфере безопасности компьютерной информации как элемент системы особенной части уголовного кодекс российской федерации / А.В. Мнацаканян // Пробелы в российском законодательстве.-2012.- № 3.-С.158-161.

14. Подольный Н. А. О некоторых источниках создания частных методик расследования преступлений // Следователь. - 2004. - № 11 (79). - С. 30-32.

15. Поляков В. В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений // Lex russica. — 2022. — Т. 75. — № 6. — С. 85–96.

16. Поляков, В.В. О необходимости криминалистической характеристики преступлений / В.В. Поляков, А.В. Шебалин // Юридическая наука и образование в России и Азии: Методика преподавания права. Материалы I Российско-Азиатского Правового Конгресса. 2-3 октября 2014 г. – Барнаул : Издательская группа «Си-пресс», 2014. – С. 382-386.

17. Поляков, В.В. Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации / В.В. Поляков // Региональные аспекты технической и правовой защиты информации : монография / В.В. Поляков, В.А. Трушев, И.А. Рева и др. – Барнаул : Изд-во Алт. ун-та, 2013. – Гл. 1. – С. 9-42.

18. Поляков, В.В. Результаты анкетирования по делам о неправомерном удаленном доступе к компьютерной информации / В.В. Поляков // Уголовно-процессуальные и криминалистические чтения на Алтае

: матер. межрегион. науч.-практ. конф. / под ред. В. К. Гавло. – Барнаул : Изд-во Алт. ун-та, 2008. – Вып. 7. – С. 245 - 249.

19. Рогозин, В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий / В.Ю. Рогозин // Расследование преступлений: проблемы и пути их решения. - 2015. - № 1 (7). - С. 56-58.

20. Шутова, А.А. Информация как конструктивный признак отдельных составов преступлений / А.А. Шутова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. - 2015.- № 2.- С.201-205.

1.4. ТЕМА 3. ПРЕДМЕТ И ОБЪЕКТ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Объект компьютерных преступлений.
2. Предмет преступных посягательств: понятие, виды.

На проведение занятия отводится 4 часа.

Дополнительная литература

1. Бессонов А. А. Объект (предмет) преступного посягательства как элемент криминалистической характеристики преступлений / А. А. Бессонов // Вестник Калмыцкого института гуманитарных исследований РАН. – 2014. - № 4. - С. 231.

2. Вехов, В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления / В.Б. Вехов // Московский государственный технический университет имени Н.Э. Баумана.-2015.-№8.-С.43-46.

3. Воробьев, В.В. К вопросу о содержании и объеме предмета преступлений в сфере компьютерной информации / В.В. Воробьев // Вестник Оренбургского государственного университета. – 2011. - № 3.- С. 66-69.

4. Воробьёв, В.В. О предмете преступления, его месте в составе преступления и особенностях в компьютерных преступлениях / В.В. Воробьев // Международный научный журнал «Символ науки». – 2015. - № 6.-С.221-223.

5. Гребеньков, А.А. Родовой объект преступлений в сфере компьютерной информации / А.А. Гребеньков // Известия Юго-Западного государственного университета. Серия: История и право. – 2012. - № 2-2. - С. 30-33.

6. Лопатина, Т.М. Особенности объекта преступлений в сфере компьютерной информации / Т.М. Лопатина // Бизнес в законе. 2006.-№1-2. - С.169-171.

7. Маляров, А.Н. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) / А.Н.Маляров // Общество и право.-2008.- №2(20).- С.140-143.

8. Сафонов, О.М. Особенности объекта уголовно-правовой охраны для преступлений, совершаемых с использованием компьютерных технологий / О.М. Сафронов // Грамота, 2014.- № 7 (45): в 2-х ч. Ч. I. С. 163-165.

9. Стяжкина, С.А. Информация как объект уголовно-правовой охраны: понятие, признаки, виды / С.А. Стяжкина // Вестник Удмуртского университета. Серия Экономика и право.- 2015. - № 2-2. - С. 157-161.

10. Трофимцева, С.Ю. Объект компьютерных преступлений в российском и европейском уголовном праве: сравнительный анализ / С.Ю. Трофимцева, Д.А. Илюшин, А.В. Линьков // Информационное противодействие угрозам терроризма. - 2015.- № 24. - С. 3-11.

11. Чирков, П.А. Об объекте преступлений в сфере компьютерной информации в российском уголовном праве / П.А. Чирков // Правовые вопросы связи.- 2012. - № 1. - С. 392-397.

12. Шутова, А.А. Информация как конструктивный признак отдельных составов преступлений / А.А. Шутова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2015. - № 2. - С. 201-205.

1.5. ТЕМА 4. ПРИЧИНЫ И УСЛОВИЯ, СПОСОБСТВУЮЩИЕ СОВЕРШЕНИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Контрольные вопросы к занятию:

1. Понятие и соотношение причин, условий и обстоятельств, способствующих совершению компьютерных преступлений.
2. Технические и организационные причины и условия, способствующие совершению компьютерных преступлений.
3. Общесоциальные, психологические и экономические причины и условия, способствующие совершению компьютерных преступлений.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Богданова, Т.Н. Причины и условия совершения преступлений в сфере компьютерной информации / Т.Н.Богданова // Вестник Челябинского государственного университета.- 2013.-№11.-С.64-67.
2. Евдокимов, К.Н. К вопросу о причинах компьютерной преступности в России / К.Н. Евдокимов // Известия Иркутской государственной экономической академии. - 2010.-№5. - С. 167-170.
3. Егорышева, Е.А. Основные обстоятельства, способствующие неправомерному доступу к компьютерной информации / Е.А. Егорышева, А.С. Егорышев // Вестник БИСТ (Башкирского института социальных технологий). - 2009. - № 3. - С. 73-82.
4. Ковалев, Д.И. Причины компьютерной преступности / Д.И. Ковалев // Вестник Академии. - 2011. - 4. - С. 122-124.
5. Коликов, Н.Л. Причины и условия профессиональной компьютерной преступности / Н.Л. Коликов // Вестник ЮУрГУ.- 2011. - № 19. – С.30-33.

6. Липинский, Д.А. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации / Д.А. Липинский, К.Н. Евдокимов // Всероссийский криминологический журнал. - 2015. Т. 9. - № 1. - С. 101-110.

7. Сизов, А.В. Причины и условия совершения преступлений в сфере компьютерной информации / А.В. Сизов // Информационное право. -2008. - № 2.- С. 38-42.

8. Шляпникова, О.В. Неосторожные компьютерные преступления: причины, последствия, профилактика / О.В. Шляпникова, К.П. Семёнов, Т.В. Семёнова // Информационная безопасность регионов. - 2010. - № 2. - С. 63-68.

1.6. ТЕМА 5. ОСОБЕННОСТИ ЛИЧНОСТИ УЧАСТНИКОВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Личность преступника, совершающего компьютерные преступления.
2. Классификации компьютерных преступников.
3. Цели и мотивы совершения компьютерных преступлений.
4. Личность потерпевшего от компьютерных преступлений.
5. Личность свидетеля компьютерного преступления.
6. Особенности преступных групп, организованных группи сообществ, совершающих компьютерные преступления.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Беляев, Е.В. Типы личности «компьютерного преступника» / Беляев Е.В. // Вестник Тюменского института повышения квалификации сотрудников МВД России.- 2013. - № 1. - С. 74-77.
2. Будаковский, Д.С. Характеристика свойств лиц, совершающих преступления в сфере компьютерной информации / Д.С. Будаковский // Вестник Российской таможенной академии.- 2009. - № 3. - С. 123-128.
3. Давыдов С.И., Кондратьев М.В., Поляков В.В. Противодействие транснациональным организованным группам, использующим информационно-коммуникационные технологии для незаконного сбыта наркотических средств // Правоприменение. – 2024. - № 8 (1). – С. 111-120.
4. Дьяков, В.В. О личности преступника, как компоненте системы криминалистической характеристики преступлений в сфере компьютерной информации / В.В. Дьяков // Бизнес в законе, - 2008.-№2.- С.129-131.

5. Евдокимов, К.Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) / К.Н. Евдокимов // Сибирский юридический вестник. - 2011.- № 1. - С. 86-90.

6. Ефремов, К.А. Личность преступника, совершающего преступления в сфере компьютерной информации / К.А. Ефремов // Общество: политика, экономика, право. - 2016. - № 6. - С. 92-95.

7. Исмаилова, М.М. Особенности психологических установок компьютерных преступников / М.М. Исмаилова // Системные технологии.- 2014.- №10. - С.66-68.

8. Ковалев, Д.И. Криминологическая характеристика личности преступника, совершающего преступление в сфере компьютерной информации / Д.И. Ковалев // Вестник Академии. - 2011. - № 3. - С. 90-92.

9. Коликов, Н.Л. Причины и условия профессиональной компьютерной преступности // Н.Л. Коликов // Вестник ЮУрГУ.- 2011. - № 19. – С.30-33.

10. Косенков, А.Н. Общая характеристика психологии киберпреступника / А.Н. Косенков, Г.А. Черный // Криминалистический журнал ОГУЭП, - 2008. - № 3(21). – С.87-93.

11. Макушев, Д.И. Криминологическая характеристика личности киберпреступника / Д.И. Макушев // Актуальные проблемы гуманитарных и естественных наук.- 2016.- № 1-3. - С. 202-204.

12. Маслакова, Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика /Е.А. Маслакова // Политика и право, -2014. -№ 1.- С. 114-121.

13. Морар, И.О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? / И.О. Морар // Российский следователь.- 2012.- № 13. - С. 34-38.

14. Осипенко, А.Л. Информационно-психологическое влияние ресурсов сети Интернет на формирование социальных установок ее

пользователей / А.Л. Осипенко // Психопедагогика в правоохранительных органах.-2006.-№3. - С.135-138.

15. Поляков В.В. Групповая форма совершения преступлений как один из признаков высокотехнологичной преступности / В.В. Поляков // Российский юридический журнал. – 2023. - № 1 (148). – С. 117-126.

16. Поляков, В.В. Характеристика личности киберпреступников / В.В. Поляков, Н.В. Людкова // Теоретические и практические проблемы организации раскрытия и расследования преступлений: сб. мат. Всерос. науч. практ. конф. 22 апреля 2016 г.; - Хабаровск: ДВЮИ МВД России. - С. 250-255.

17. Попов, К.И. Личность преступника, совершающего преступления в сфере компьютерной информации / К.И. Попов // НаукаЮУрГУ: материалы 66-й научной конференции. Секции социально-гуманитарных наук. – С.1731-1738.

18. Сухих, И.И. Взаимосвязь личности преступника и совершенного им преступления в сфере компьютерной информации / И.И. Сухих // Вестник УрФО. Безопасность в информационной сфере.-2013.-№ 1.-С.22-14.

19. Тулегенов, В.В. Киберпреступность как форма выражения криминального профессионализма / В.В. Тулегенов // Криминология: вчера, сегодня, завтра. – 2014.- №2(33).- С. 94-97.

1.7. ТЕМА 6. СПОСОБЫ И МЕХАНИЗМЫ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Понятие и разновидности способов совершения компьютерных преступлений.
2. Подготовка к совершению компьютерных преступлений.
3. Непосредственное совершение компьютерных преступлений.
4. Сокрытие следов компьютерных преступлений и участия в нем.
5. Классификации способ совершения компьютерных преступлений.
6. Относительно простые способы совершения компьютерных преступлений.
7. Высокотехнологичные способы совершения компьютерных преступлений.
8. Понятие и виды механизмов совершения компьютерных преступлений.

На проведение занятия отводится 6 часов.

Дополнительная литература

1. Абдусаламов, Р.А. Специфика и способы совершения преступлений в сети интернет / Р.А Абдусаламов, Ш.Д. Арсланов // Юридический вестник ДГУ. - 2014.- № 1. - С. 116-118.
2. Горбаруков, В.А. О некоторых способах совершения преступлений против собственности с использованием эвм / В.А. Горбаруков// Вестник Северо-Кавказского федерального университета. - 2011. - № 1. - С. 182-183.
3. Горбунов, А.Н. Способы незаконного использования пластиковых карт при совершении преступлений / А.Н. Горбунов, В.Н. Цимбал // Общество и право. - 2013. - № 3 (45). - С. 217-221.

4. Журкина, О.В. К вопросу о способах совершения мошенничества с использованием сотовой (подвижной) связи / О.В. Журкина, И.В. Бондаренко // Вопросы российского и международного права. - 2015. - № 3-4. - С. 19-30.

5. Косынкин, А.А. Соотношение способа совершения и способа противодействия расследованию преступлений / А.А. Косынкин // Актуальные проблемы гуманитарных и естественных наук. - 2014. - № 2-2. - С. 61-63.

6. Лямцев, А.Н. Мобильные коммуникационные устройства и их использование в противоправных целях / А.Н. Лямцев // Вопросы современной науки и практики. Университет им. В.И. Вернадского. - 2014.- № 4 (54).- С. 200-204.

7. Ляшко, А.А. Обман и злоупотребление доверием как главнейшие признаки отличия мошенничества от гражданско-правовой ответственности / А.А. Ляшко, И.П. Иванов // Актуальные направления научных исследований: от теории к практике. - 2015. - № 3 (5). - С. 497-500.

8. Малышкин, П.В. Способы сокрытия преступлений, совершаемых с применением информационных компьютерных технологий / П.В. Малышкин // Вестник Мордовского университета. - 2014. Т. 24. - № 4. - С. 42-47.

9. Николаев, В.Ю. Способы совершения компьютерных преступлений и использование компьютерных (информационных) технологий как способ совершения преступления / В.Ю. Николаев // Правовая идея. - 2013. - № 4 (4). - С. 6.

10. Поляков В. В. Структура и содержание способа совершения высокотехнологичных преступлений / В.В. Поляков // Российское право: образование, практика, наука. - 2023. - № 1. - С. 27–39.

11. Поляков В.В. Криминалистическая классификация способов противодействия расследованию высокотехнологичных преступлений / В.В.

Поляков // Юридическая наука и правоохранительная практика. – 2023. - № 1 (63). – С. 69-79.

12. Поляков, В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации / В.В. Поляков, С.М. Слободян // Известия Томского политехнического университета. – 2007. – Т. 310, № 1. – С. 212 – 216.

13. Поляков, В.В. Классификация способов совершения преступлений в сфере компьютерной информации / В.В. Поляков, Е.Г. Смирнов // V Пленум СибРОУМО (Сибирского регионального отделения учебно-методического объединения) вузов России по образованию в области информационной безопасности. XIII Всерос. конф. «Проблемы информационной безопасности государства, общества и личности»: 5-9 июня 2012г.: Томск-Новосибирск. – Томск: Изд-во «В-Спектр», 2012. – С. 108 - 109.

14. Поляков, В.В. Криминалистические особенности бесконтактного способа совершения наркопреступлений / В.В. Поляков, М.В. Кондратьев // Известия Алтайского государственного университета. – 2015. –№ 2 (86). – С. 83-86.

15. Поляков, В.В. О высокотехнологичных способах совершения преступлений в сфере компьютерной информации / В.В. Поляков // Уголовно-процессуальные и криминалистические чтения на Алтае: матер. ежег. Всеросс. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета. – Барнаул: Изд-во Алт. ун-та, 2012. – Вып. 11-12. – С.123 - 126.

16. Поляков, В.В. Особенности стадии подготовки к преступлениям в сфере компьютерной информации / В.В. Поляков, Г.А. Кацюка // Ломоносовские чтения на Алтае: Фундаментальные проблемы науки и образования: матер. Междунар. молодежной школы-семинара (Барнаул, 11-14 ноября 2014 г.). – Барнаул : Изд-во Алт. ун-та, 2014. – С. 2577-2578.

17. Поляков, В.В. Типичные способы совершения преступлений, связанных с неправомерным доступом к компьютерной информации / В.В. Поляков // Сборник материалов криминалистических чтений 2005-2006 гг. / под ред. Ю.Л. Бойко. – Барнаул: Изд-во БЮИ МВД России, 2006. – С. 96 - 97.

18. Смагоринский, Б.П. О способах совершения мошенничеств с использованием сотовой связи Б.П. Смагоринский, М.С. Дьяконов, М.С. Дронова // Вестник Волгоградской академии МВД России.- 2014.- № 2 (29). - С. 98-104.

19. Шиловский, С.В. О месте способа совершения преступления в преступлении и составе преступления / С.В. Шиловский // Вестник Северного (Арктического) федерального университета. Серия: Гуманитарные и социальные науки. - 2014. - № 2. - С. 109-113.

1.8. ТЕМА 7. ОБСТАНОВКА СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Понятие обстановки совершения компьютерных преступлений.
2. Материальная, социальная и иная обстановка совершения компьютерных преступлений.
3. Благоприятная и неблагоприятная обстановка совершения компьютерных преступлений.
4. Место подготовки к компьютерным преступлениям. Место совершения компьютерных преступлений. Место сокрытия компьютерных преступлений.
5. Транснациональная специфика совершения компьютерных преступлений.
6. Особенности мест происшествия по длящимся и эпизодическим компьютерным преступлениям.
7. Время совершения компьютерных преступлений.

На проведение занятия отводится 6 часов.

Дополнительная литература

1. Введенская, О.Ю. Обстановка совершения интернет-преступлений / О.Ю. Введенская // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. - 2015.- № 1. - С. 41-45.
2. Поляков, В.В. Место происшествия как элемент криминалистической характеристики компьютерных преступлений / В.В. Поляков // Юридическая наука и образование в России и Азии. Методика преподавания права. Материалы I Российско-Азиатского Правового

Конгресса. 2-3 октября 2014 г. – Барнаул: Издательская группа «Си-пресс», 2014. – С. 371-375.

3. Поляков, В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия Алтайского государственного университета.-2013.-Выпуск № 2 (78) / том 1.-С.114-115.

4. Степанов-Егиянц, В.Г. К вопросу о месте совершения компьютерных преступлений / В.Г. Степанов-Егиянц // Научно-информационный журнал армия и общество.-2014.-№5 (42). - С.16-20.

5. Шевченко, И.С. Киберпространство как элемент обстановки совершения преступлений / И.С. Шевченко, Н.Н. Михайлюченко // Академический юридический журнал. - 2015. - № 1 (59).- С.52 - 59.

1.9. ТЕМА 8. СРЕДСТВА СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Средства подготовки к компьютерным преступлениям.
2. Средства непосредственного совершения компьютерных преступлений.
3. Средства сокрытия компьютерных преступлений.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Вехов, В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления / В.Б. Вехов // Московский государственный технический университет имени Н.Э. Баумана.-2015.-№8.-С.43-46
2. Демин, К.Е. Криминалистические аспекты получения доказательственной информации с электронных носителей данных / К.Е.Демин, А.А.Васильев // Публичное и частное право.-2011.-№3.-С.147-161.
3. Лапин, С.А. Программное обеспечение как средство совершения компьютерных преступлений / С.А. Лапин, В.В. Поляков // Ползуновский альманах. - 2016. - №2. – С. 201-204.
4. Поляков В.В. Применение технологий социальной инженерии при совершении высокотехнологичных преступлений // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. 2023. – Т. 27. – № 3. – С. 175- 188.
5. Поляков В.В. Тенденции развития цифровых средств совершения высокотехнологичных преступлений / В.В. Поляков // Информационное право. – 2023. - №4 (78). – С. 26-28.

6. Поляков, В.В. Использование сети интернет при совершении преступлений против детей / В.В. Поляков, А.С. Мананников // Сборник материалов криминалистических чтений. – 2014. - № 10. - С. 113-114.

7. Поляков, В.В. Программное обеспечение, используемое для совершения компьютерных преступлений / В.В. Поляков, С.А. Лапин // Ломоносовские чтения на Алтае–2013: матер. Междунар. молодежной школы-семинара (Барнаул, 5-8 ноября 2013 г.). – Барнаул: Изд-во Алт. ун-та, 2013. – Ч. 2 . – С. 15-17.

8. Поляков, В.В. Средства совершения компьютерных преступлений / В.В. Поляков, С.А. Лапин // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2014. - № 2 (32). - С. 162-166.

9. Старичков, М.В. Вопросы использования носителей компьютерной информации в качестве доказательств / М.В. Старичков // Известия тульского государственного университета: экономические и юридические науки. - 2014.- №2(5).- С.114-125.

10. Холопова, Н.А. Поляков В.В. Использование сетевых информационных технологий в экстремистской деятельности / Н.А. Холопова, В.В. Поляков // Организационное, процессуальное и криминалистическое обеспечение уголовного производства : материалы VI Международной научной конференции студентов и магистрантов, 15 декабря 2017 года, Симферополь / отв. ред. М. А. Михайлов, С.А. Поляков, Е.А. Ануфриева, Т. В. Омельченко. – Симферополь : ИТ «АРИАЛ», 2017. – С. 123-125.

1.10. ТЕМА 9. СЛЕДОВАЯ КАРТИНА КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Понятие и специфика следов компьютерных преступлений (виртуальных, электронно-цифровых, компьютерных).
2. Классификация следов компьютерных преступлений.
3. Особенности механизма их следообразования.
4. Следовая картина компьютерных преступлений.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Введенская, О.Ю. Особенности следообразования при совершении преступлений посредством сети интернет / О.Ю. Введенская // Юридическая наука и правоохранительная практика. - 2015. - № 4 (34). - С. 209-216.

2. Гавло, В.К. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации / В.К. Гавло, В.В. Поляков // Российский юридический журнал. – 2007. – №5 (57). – С. 146-152.

3. Гавло, В.К. Следовая картина преступлений, связанных с неправомерным доступом к компьютерной информации с помощью удаленно расположенной ЭВМ, и ее значение для производства судебных компьютерно - технических экспертиз / В.К. Гавло, В.В. Поляков // Теория и практика судебных экспертиз в современных условиях: сб. матер. Междунар. науч.-практ. конф. – М.: ТК Велби, Изд-во Проект, 2007. – С. 471 - 475.

4. Коновалова, А.Б. К вопросу о тактико-процессуальных основах установления следов преступления в высокотехнологичной сфере / А.Б. Коновалова // Наука и образование.-2016.-№ 1 (3).-С.113-116.

5. Косынкин, А.А. Инсценировка как форма противодействия расследованию преступлений в сфере компьютерной информации / А.А. Косынкин // Вестник челябинского государственного университета. Серия: Право - 2011. -№29. - С. 78-80.

6. Косынкин, А.А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А.А. Косынкин // Российский следователь.- 2012.- № 2.

7. Косынкин, А.А. Соотношение способа совершения и способа противодействия расследованию преступлений / А.А. Косынкин // Актуальные проблемы гуманитарных и естественных наук. - 2014. - № 2-2. - С. 61-63.

8. Мочагин, П.В. Виртуально-информационный и невербальный процесс отражения следообразований как новое направление в криминалистике и судебной экспертизе /П.В. Мочагин // Вестник Удмуртского университета.-2013.-№ 2.- С.148-154.

9. Осипенко, А.Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс/ А.Л. Осипенко // Научный вестник Омской академии МВД России.-2009.- № 4(35).

10. Поляков, В.В. Изучение виртуальных следов преступлений, связанных с неправомерным доступом к компьютерной информации / В.В. Поляков, С.В. Кучерявский // Ползуновский альманах. – 2006. – №4. – С. 55 - 58.

11. Поляков, В.В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике / В.В. Поляков, А.В. Шебалин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: матер. одиннадцатой Междунар. науч.-практ. конф. в 2-х частях. – Барнаул: Барнаульский юридический институт МВД России, 2013. – Ч. 1. – С. 123-125.

1.11. ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1.Основные понятия информационной безопасности и компьютерных преступлений. Понятие компьютерной информации.

2.Понятие компьютерных преступлений, соотношение с понятием преступления в сфере компьютерной информацией.

3.Проблемы выработки определений: электронных доказательств; электронных документов; электронно-цифровых (виртуальных) следов.

4.Понятие и содержание уголовно-правовой характеристики компьютерных преступлений. Понятие и содержание криминалистической характеристики компьютерных преступлений. Соотношение данных характеристик.

5.Проблема подразделения элементов криминалистической характеристики компьютерных преступлений.

6.Соотношение причин, условий и обстоятельств и условия, способствующих совершению компьютерных преступлений. Технические причины и условия, способствующие совершению компьютерных преступлений.

7.Организационные причины и условия, способствующие совершению компьютерных преступлений.

8.Общесоциальные причины и условия, способствующие совершению компьютерных преступлений.

9.Экономические причины и условия, способствующие совершению компьютерных преступлений.

10.Психологические причины и условия, способствующие совершению компьютерных преступлений.

11.Личность преступника, совершающего компьютерные преступления. Классификации компьютерных преступников.

12.Цели и мотивы совершения компьютерных преступлений. Личность потерпевшего от компьютерных преступлений.

13.Личность свидетеля компьютерного преступления. Характеристика преступной группы или сообщества.

14.Объект компьютерных преступлений. Предмет преступных посягательств: понятие, виды

15.Зависимости личности преступника и избираемых им средств совершения преступления.

16.Зависимости предмета преступных посягательств и личности преступника.

17.Зависимости обстановки совершения компьютерных преступлений и выбора на выбор способа совершения компьютерных преступлений.

18.Зависимости средств совершения компьютерных преступлений и способа совершения компьютерных преступлений.

19.Понятие обстановки совершения компьютерных преступлений. Материальная, человеческая и иная обстановка совершения компьютерных преступлений.

20.Благоприятная и неблагоприятная обстановка совершения компьютерных преступлений. Время совершения компьютерных преступлений.

21.Место подготовки к компьютерным преступлениям. Место совершения компьютерных преступлений. Место сокрытия компьютерных преступлений.

22.Средства подготовки к компьютерным преступлениям.

23.Средства непосредственного совершения компьютерных преступлений.

24.Средства сокрытия компьютерных преступлений.

25.Понятие следов (виртуальных, электронно-цифровых) и следовой картины компьютерных преступлений.

26.Классификации следов компьютерных преступлений.

27.Характер и размер вреда, причиненного преступлением.

28.Понятие способов совершения компьютерных преступлений.

29.Подготовка к совершения компьютерных преступлений.

30.Непосредственное совершение компьютерных преступлений.

31.Сокрытие следов компьютерных преступлений и участия в нем.

32.Классификации способ совершения компьютерных преступлений.

33.Высокотехнологичные способы совершения компьютерных преступлений.

1.12. ТЕМЫ РЕФЕРАТОВ И НАУЧНЫХ ДОКЛАДОВ

1. Понятийный аппарат в сфере компьютерных преступлений
2. Характеристика компьютерных преступлений
3. Причины и условия, способствующие совершению преступлений в сфере компьютерной информации.
4. Особенности личности основных участников события компьютерного преступления.
5. Предмет и объект компьютерных преступлений
6. Способы и механизмы совершения компьютерных преступлений.
7. Обстановка и время совершения компьютерных преступлений.
8. Место происшествия по компьютерным преступлениям.
9. Средства совершения компьютерных преступлений.
10. Следовая картина преступлений в сфере компьютерной информации.
11. Корреляционные взаимосвязи элементов криминалистической характеристики компьютерных преступлений.

ГЛАВА 2. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

2.1. Теоретические основы расследования и доказывания компьютерных преступлений

Методика расследования компьютерных преступлений может быть представлена как многоуровневая система, состоящая из двух подсистем: криминалистической характеристики преступления и криминалистической характеристики расследования преступления. Если криминалистическая характеристика преступлений содержит «наиболее существенные признаки, отличительные свойства по совершению отдельных видов и групп преступлений»[11], то криминалистическая характеристика расследования преступлений, содержит основные признаки деятельности по расследованию преступлений. В ней могут быть выделены следующие подсистемы, характеризующие: проверочный этап; предварительное расследование; судебное разбирательство; возобновления производства по новым или вновь открывшимся.

Наименее разработанными и одновременно одними из наиболее сложных являются вопросы доказывания преступлений, совершенных в сфере компьютерной информации. В большей степени это относится к стадии судебного разбирательства. Рассмотрение проблем и особенностей доказывания особенно актуально в связи с неадаптированностью действующего материального и, в еще большей степени, уголовно-процессуального законодательства к новым способам совершения компьютерных преступлений. При этом расследование компьютерных преступлений осложняется недостаточностью криминалистических методик в

[11] Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений: монография. Томск: Изд-во Томского ун-та, 1985. С. 162.

целом и отдельных рекомендаций по обнаружению, оценке, исследованию и использованию доказательств в частности. В большей степени это относится к сложностям расследования быстро развивающейся высокотехнологичной преступности[12].

Процесс доказывания является основой установления истины по уголовному делу. Доказывание совершения преступления строится на преимущественном оперировании полученными в ходе следствия доказательствами[13]. При этом, доказательство как уголовно-процессуальная категория представляет собой систему взаимосвязанных и взаимообусловленных элементов и возникающих в связи с их формированием отношений. В качестве элементов выступают фактические данные (то есть сведения о фактах); источники фактических данных; способы и порядок собирания, закрепления и проверки этих фактических данных и их источников[14]. Посредством доказательств, как отмечает И.М. Лузгин, в расследовании достигается переход от познания явлений к раскрытию их сущности, установлению связей между действиями лица и его последствиями[15]. Анализ судебно-следственной практики показал, что имеется объективно существующая проблема, которую приходится преодолевать в ходе предварительного и судебного следствия. Она заключается в сложившейся у субъектов доказывания ориентации на традиционные доказательства, в то время как доказательства, собранные при расследовании компьютерных преступлений имеют специфику, вытекающую из преимущественно электронно-цифрового характера следов преступления.

---

[12] 125. Поляков В.В. К проблеме криминалистической сложности расследования высокотехнологичных преступлений / В.В. Поляков // Российский следователь. - 2023. - № 11. - С. 7-10.

[13] Белкин, Р.С. Криминалистика и доказывание / Р.С. Белкин, А.И. Винберг. – М.: Юрид. лит., 1969. – 216 с.

[14] Балакшин, В.С. Доказательства в теории и практике уголовно-процессуального доказывания (важнейшие проблемы в свете УПК Российской Федерации): автореф. дис. … д-ра юрид. наук / В.С. Балакшин. - Екатеринбург, 2005. - С. 12-13.

[15] Лузгин, И.М. Методологические проблемы расследования / И.М. Лузгин. – М.: Юрид. лит., 1973. – С. 179.

Кроме того, процесс доказывания в случае преступлений в сфере компьютерной информации, и без того отличающийся большой сложностью и спецификой, затрудняется крайне слабой разработанностью вопросов, связанных с применимостью, относимостью и допустимостью используемых электронных доказательств. Отметим, что в криминалистической теории эти вопросы являются дискуссионными и мнения по ним отражают различные, зачастую противоположные, точки зрения авторов[16].

Из Уголовно-процессуального кодекса РФ следует, что проверка доказательств производится следователем, прокурором и судьей путем сопоставления их с другими доказательствами, которые имеются в деле, и установлении их источников. Оценка доказательств связана с логической мыслительной деятельностью при переработке и получении новой информации[17]. В результате этой деятельности устанавливаются фактические обстоятельства дела и делается вывод о доказанности или недоказанности фактов, а также достоверности оцениваемых доказательств.

В суде подлежат доказыванию следующие обстоятельства: событие преступления; объект; предмет; способ; место, время; причиненный ущерб; виновные лица; состав группы и роль ее участников (если она имелась); какие обстоятельства способствовали совершению преступления, а также должна быть установлена причинно-следственная связь между действиями, входящими в способ совершения преступления, и наступившими противоправными последствиями.

Представляется необходимым определиться с видами доказательств,

---

[16] Мылицын, Р.Н. Электронное сообщение как доказательство в уголовном процессе [Электронный ресурс] / Р.Н. Мылицын. – Электрон. дан. -Режим доступа: http://nadzor.pk.ru/analit/show_a.php?id=667, свободный; Вехов, В.Б. Проблемы расследования преступлений в сфере компьютерной информации / В.Б. Вехов // Современные проблемы криминалистики: межвуз. сб. науч. тр. – Волгоград: Изд-во ВЮИ МВД России, 1999. – С. 176 – 180; Мещеряков, В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ / В.А. Мещеряков. – Воронеж: Изд-во Воронеж. гос. ун-та, 2001. - 176 с.

[17] Белкин, Р.С. Ленинская теория отражения и методологические проблемы советской криминалистики / Р.С. Белкин. – М.: ВШ МВД СССР, 1970. – С. 25.

которые могут использоваться в судебном процессе по делам о преступлениях в сфере компьютерной информации. К доказательствам отнесятся: показания подозреваемого, обвиняемого, показания потерпевшего, свидетеля; заключение и показания эксперта; заключение и показания специалиста; вещественные доказательства; протоколы следственных и судебных действий; иные документы. В случае преступлений в сфере компьютерной информации решающее значение имеют электронные доказательства[18]. В соответствии с приведенным в УПК РФ перечнем электронные доказательства наиболее близки к понятию «иные документы». Это связано с тем, что они имеют вид электронных файлов (документов), находящихся на носителе информации, содержащих сведения о событии преступления, например, о способе, времени, средствах совершения преступления и иных данных, связанных с преступлением, посредством которых происходит доказывание.

Для криминалистической науки и практики важно избавиться от несовершенства понятийного аппарата, используемого при работе с электронными доказательствами.

Основой для решения этого вопроса, на наш взгляд, может служить исходная позиция, выраженная в работе А.М. Баранова при анализе использования доказательств, полученных с помощью средств электронно-вычислительной техники: «Сегодня необходимо, чтобы форма не мешала технологии процесса, а устанавливала общие правила производства и сбора доказательств, обеспечивала право лиц на определенном этапе производства»[19]. Наиболее адекватной развитию криминалистической теории и судебно-следственной практики для характеристики формы электронных доказательств является понятие «электронный документ». Согласно

[18] Зайцев, П. Электронный документ как источник доказательств / П. Зайцев // Законность. - 2002. – № 4. – С. 40 – 44; Вершинин, А.П. Электронный документ: правовая форма и доказательство в суде: учеб.- практ. пособие / А.П. Вершинин. - М.: Городец, 2000. - С. 40.

действующему законодательству, «электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»[20].

Определение понятий «электронный документ» и «электронное доказательство» вызывает дискуссии в криминалистике. В нормативно-правовых актах и руководящих разъяснениях судам для обозначения формы представления компьютерной информации используются различные термины, такие как: «электронный документ», «документ, подготовленный с помощью электронно-вычислительной техники», «машинный документ»[21]. Под электронным документом В.Б. Вехов понимает «сведения о лицах, предметах, фактах, событиях, явлениях и процессах в электронно-цифровой форме, зафиксированных на машинном носителе с помощью электромагнитных сигналов с реквизитами, позволяющими идентифицировать данные сведения»[22]. Интересной представляется точка зрения В.А. Мещерякова[23], который предлагает расширить понятие «электронный документ» и заменить его на понятие «электронный цифровой объект», при этом сам автор выражает сомнение в готовности законодателя принять его предложение.

Электронный документ, содержащий компьютерную информацию,

[20] Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 06.04.2011 N 63-ФЗ (ред. от 04.08.2023). Ст. 2.

[21] Зайцев, П. Электронный документ как источник доказательств / П. Зайцев // Законность. - 2002. – № 4. – С. 40 – 44.

[22] Вехов, В.Б. Основные направления развития криминалистического исследования компьютерной информации и ее материальных носителей / В.Б. Вехов // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники: проблемы, тенденции, перспективы: Матер. Всерос. конф. - М.: МАКС Пресс, 2005. – С. 11-13.

[23] Мещеряков, В.А. Электронные цифровые объекты в уголовном процессе и криминалистике / В.А. Мещеряков // Воронежские криминалистические чтения: сб. науч. тр. / под ред. О.Я. Баева. - Воронеж: Изд-во Воронеж. гос. ун-та, 2004. - Вып. 5. - С. 153 – 169.

может быть использован в качестве электронного доказательства лишь при точном указании источников этой информации. В качестве источников могут выступать накопители на магнитных и оптических (лазерных) дисках, большая группа всевозможных съемных устройств (включая флэш-память и телекоммуникационные устройства связи), оперативное запоминающее устройство (ОЗУ), и постоянное запоминающее устройство (ПЗУ) компьютера, блоки памяти периферийных устройств (принтеров, многофункциональных устройств и т.д.)

Отдельно в силу проблем, возникающих в процессе расследования, подчеркнем, что электронный документ приобретает силу электронного доказательства только при его соответствии требованиям допустимости, относимости и достоверности. Однако реализация этого положения, в условиях существующего Уголовно-процессуального кодекса РФ, затруднительна. Практика показывает, что правоохранительные органы на предварительном следствии могут допустить ошибки, в результате которых теряются сведения и сообщения, которые могли бы иметь доказательственное значение. В ходе судебного расследования такие ошибки приводят к недопустимости, а также недостоверности или неотносимости представленных доказательств.

С другой стороны, следователи по делам о преступлениях в сфере компьютерной информации нередко допускают процессуальные и тактические упущения и ошибки. В связи с этим на судебном следствии могут возникнуть сложности, вызванные отсутствием определенных материалов следственных действий, которые не были произведены следователем, посчитавшим их проведение нецелесообразным. Эти обстоятельства придают особую важность правильно организованной проверке поступающей к субъекту доказывания информации, ее

квалифицированной оценке в целях принятия соответствующего решения[24].

На практике «при наличии нескольких средств доказывания письменным документам отдается предпочтение, ввиду надежности их исследования и простоты непосредственного восприятия органами чувств человека»[25]. С таким положением дел нельзя согласиться, поскольку, как справедливо указывает Р.Г-В. Локк, «информация, полученная с помощью технического средства, более полно и точно отражает объективную реальность, нежели информация, отображенная в человеческом сознании как целостный образ, перенесенный затем в виде знаков алфавита на бумагу»[26].

В настоящее время даже опытные судьи и участники судебного процесса оказываются не готовыми к разрешению сложных ситуаций, основанных на специфике компьютерной информации и средствах компьютерной техники. В результате выносимые судебные решения отличаются недостаточной аргументированностью и противоречивостью. Так, был отменен оправдательный приговор суда в связи с неправильным представлением о том, что следует относить к компьютерной информации, средствам ее обеспечения, какая информация является охраняемой законом. Суд г. Минусинска решил, что К., имевший служебный доступ к серверу организации, установил в его операционную систему дополнительную программу, которая не приводила к незаконному воздействию на компьютерную информацию, а находилась в доступе только со средствами ее обеспечения. Красноярский краевой суд справедливо придерживался иного мнения, полагая, что операционная система является ничем иным, как совокупностью данных и команд, то есть представляет собой компьютерную информацию. Данная компьютерная информация приобреталась специально для целей организации и была оснащена системами безопасности,

[24] Кручинина, Н.В. Основы криминалистического учения о проверке достоверности уголовно-релевантной информации: автореф. дис. … канд. юрид. наук / Н.В. Кручинина. - Москва, 2003. – С. 15.

[25] Локк, Р.Г-В. Процессуальная сущность документов и иных носителей информации / Р.Г-В. Локк // Следователь. – 2004. - № 9. – С. 18.

[26] Там же. С. 18.

препятствующими получению к ней доступа со стороны посторонних лиц. Следовательно, программа, установленная на сервер К., представляет собой компьютерную информацию, воздействующую на охраняемую законом компьютерную информацию организации[27].

Отдельного рассмотрения заслуживает вопрос об объектах носителях следов преступлений. Такие объекты должны изыматься в оригинале в натуре. Таким образом, они изымаются в приоритетном порядке по сравнению с их копями, слепками и т.п. Однако носители компьютерной информации обладают спецификой. В ранее действовавшей редакции ст. 272 УК РФ определялось, что компьютерная информация находится на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Соответственно, изъять информацию вместе с носителем не всегда представлялось возможным. В ныне действующей редакции от этого уточнения законодатель отказался, но пояснил, что: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Отсюда можно сделать вывод, что конкретное (поименное) перечисление носителей компьютерной информации нецелесообразно в силу их неопределенного и увеличивающегося числа. Типичными носителями информации могут выступать: CD – диски, флэш-память, сотовые телефоны, цифровые диктофоны и аудио-плееры и иные устройства. Укажем также, что машинный носитель и компьютер в определенных случаях сами могут выступать в качестве традиционных вещественных доказательств (например, когда на них преступником оставлены следы - пальцев, инструментов и т.п.).

Осложняет работу с электронным документом, выступающим в качестве доказательства, отсутствие его однозначной привязки к конкретному

[27] Уголовное дело № 13127428 // Архив суда г. Минусинска. 2005 г.

носителю компьютерной информации[28]. Это означает, что один и тот же документ может находиться на разных носителях (например, на жестком диске компьютера и одновременно – на лазерном диске). По данному вопросу существуют разные точки зрения. Так, по мнению Р.Н. Мылицина, «не применимо сочетание таких терминов, как оригинал и копия - могут лишь существовать идентичные по своему содержанию копии одного электронного документа на разных носителях, отличающиеся между собой разве что датой создания»[29]. Отличие материальных документов от электронных проявляется в том, что любые два материальных объекта имеют физические различия, поэтому практически всегда можно установить, какой из них является оригиналом, а какой – копией (например, с помощью экспертного исследования можно определить, какой из них был создан раньше). Электронные документы многими традиционными физическими характеристиками не обладают и могут казаться идентичными. Тем не менее, и в отношении электронных документов оригинал всегда существует, это исходная (первоначально появившаяся) версия документа. Если они имеют одинаковые реквизиты, то достоверный ответ на вопрос о том, какой из них был создан раньше, получить не удастся, так как имеющиеся программные средства не всегда могут достоверно установить действительный срок создания документа. Более того, даже при различии реквизитов документов в виде даты и времени их создания достоверно полагать, что тот из них, который был создан раньше, действительно является оригиналом, нельзя, так как дата и время создания документа в основном определяются настройками компьютера и могут не отражать действительность или быть сознательно изменены. Указанную особенность электронных документов необходимо специально учитывать при доказывании по делам о преступлениях в сфере компьютерной информации.

[28] Мылицын, Р.Н. Электронное сообщение как доказательство в уголовном процессе [Электронный ресурс] / Р.Н. Мылицын. – Электрон. дан. - Режим доступа: http://nadzor.pk.ru/analit/show_a.php?id=667, свободный.

[29] Там же.

В настоящее время по-прежнему принятие электронных доказательств в суде затруднено из-за недостаточной разработанности законодательства, не успевающего за изменениями научно-технического прогресса, отражающегося на компьютерной преступности. Сложившиеся противоречия и неопределенности затрудняют процесс доказывания.

Очевидно, что наряду с электронными доказательствами в судебном процессе по делам о преступлениях в сфере компьютерной информации должны использоваться и традиционные доказательства, а именно: объяснения сторон и третьих лиц в ходе допросов, устные и письменные показания свидетелей, письменные доказательства, вещественные доказательства, заключения экспертов и специалистов и иные документы, а также результаты следственных действий, например, предъявлений для опознания, очной ставки, следственного эксперимента и других[30]. В качестве вещественных доказательств по делам о преступлениях в сфере компьютерной информации часто выступают жесткие диски и иные носители информации[31]. В теории криминалистики тактика следственных действий и использования полученных в ходе их производства традиционных доказательств освещены на достаточно высоком уровне[32].

Качественное доказывание по преступлениям в сфере компьютерной информации осложнено также недостаточной разработанностью современных положений теории идентификации. В этой связи Д.А. Степаненко пишет: «Последние 15-20 лет войдут в историю развития теории криминалистической идентификации в России как время упущенных

[30] Белкин, А.Р. Теория доказывания в уголовном судопроизводстве / А.Р. Белкин. – М.: Норма, 2005 – 528 с.; Курс криминалистики: Особенная часть. Т. 1 / отв. ред. В.Е. Корноухов. – М.: Юристъ, 2001. – С. 13-63, 149-165.

[31] Васильев, А.А. Исследование результатов экспертизы компьютерных и электронных средств при расследовании преступлений / А.А. Васильев // Закон и право. – 2002. - № 9. – С. 74.

[32] Баев, О.Я. Тактика следственных действий: учеб. пособие / О.Я. Баев. – Воронеж: Изд-во ВГУ, 1992. – 208 с.; Васильев, А.Н. Следственная тактика / А.Н. Васильев. – М.: Юрид. лит., 1976. – 200 с.; Щерба, С.П. Расследование и судебное разбирательство по делам лиц, страдающих физическими или психическими недостатками / С.П. Щерба. – М.: Юрид. лит., 1975. – 144 с.

возможностей в период застоя»[33]. Как отмечает В.Я. Колдин, особенно это проявляется в отношении «новых форм и механизмов правонарушений, опирающихся на использование современных компьютерных, информационных, промышленных и иных высоких технологий»[34].

Следует отметить, что криминалистические работы исследователей данной сферы в силу объективных причин подвержены достаточно быстрому устареванию. Некоторые тактические и технические рекомендации устарели, другие потеряли свою актуальность. Так, развитие сетевых технологий привело к повсеместному применению беспроводных технологий передачи компьютерной информации, активно развиваются технологии машинного обучения, а также развиваются квантовые технологии и робототехника[35]. Следовательно, на повестке дня стоят задачи по криминалистическому прогнозированию[36] и изучению потенциальных объектов преступных посягательств и средств совершения преступлений, а также использование новых технологий для усиления криминалистической деятельности[37].

Далее приводимые учебно-методические материалы содержат указания, рекомендации и иную информацию по проведению занятий по учебной дисциплине «Особенности расследования компьютерных преступлений». Даны примерные планы семинарских занятий и примерный перечень вопросов для самоконтроля и зачета, представлены темы для подготовки учащимися рефератов и научных докладов, по каждой из тем приведена

[33] Степаненко, Д.А. Проблемы теории и практики криминалистической идентификации: автореф. дис. … д-ра юрид. наук / Д.А. Степаненко. – Иркутск, 2006. – С 4.

[34] Колдин, В.Я. Судебная идентификация / В.Я. Колдин. – М.: ЛексЭст, 2002. – С. 10.

[35] Поляков В.В. Тенденции развития цифровых средств совершения высокотехнологичных преступлений / В.В. Поляков // Информационное право. – 2023. - №4 (78). – С. 26-28.

[36] Акиев А.Р. Развитие научных представлений о криминалистическом прогнозировании // Вестник Санкт-Петербургского университета МВД России. - 2023. - № 4 (100). - С. 80-86.

[37] Поляков В.В. Криминалистическая классификация средств высокотехнологичных преступлений / В.В. Поляков // Вестник Санкт-Петербургского университета. Право. – Т 15. - № 2. - С. 421-439.

необходимая для подготовки литература. Учебно-методические материалы рассчитаны в первую очередь на обучающихся, имеющих минимальное юридическое образование, могут быть использованы слушателями курсов повышения квалификации по юридическим направлениям подготовки.

Темы семинарских занятий отражают последовательность изучения курса и позволяют наиболее полно изучить учебный материал. Дисциплина имеет преимущественно прикладной характер и призвана привить практические навыки разрешения сложных ситуаций расследования компьютерных преступлений.

К каждой теме практического занятия приводятся контрольные вопросы и подробный список дополнительной литературы, которая рекомендуется для изучения. Выбор литературы к теме семинарского занятия определяется необходимостью более глубокого изучения отдельных вопросов темы, обращения к различным научным взглядам.

В некоторых темах курса следует изучить материалы судебной практики расследования компьютерных преступлений, необходимые для получения аналитических выводов и обобщения правоприменительной практики. Эти материалы необходимы для анализа и обобщения правоприменительной практики, позволяя выявлять ошибки следствия и эффективные приемы расследования компьютерных преступлений.

Специфика курса «Особенности расследования компьютерных преступлений» предполагает целесообразность использования компьютерной техники для наглядного представления об отдельных технических аспектах совершения компьютерных преступлений и оставляемых при этом электронно-цифровых следах, а также криминалистических рекомендациях, применяемых при расследовании данных преступлений.

В ходе изучения данной дисциплины приобретаются практикоориентированные знания, умения и навыки по использованию криминалистических средств и методов расследования компьютерных преступлений.

При обучении по учебной дисциплине «Особенности расследования компьютерных преступлений» рекомендуется использовать следующие формы работы: лекции, семинары, научные доклады, рефераты, анкетирование, решение задач, тестирование, подготовка научных публикаций, сбор судебной практики и специализированной литературы.

По итогу изучения курса «Особенности расследования компьютерных преступлений» рекомендуется экзамен как форма контроля. В качестве промежуточного контроля предусмотрено выполнение индивидуальных научно-практических заданий и тестирование по отдельным темам. В качестве промежуточного контроля предусмотрено выполнение индивидуальных научно-практических заданий и тестирование.

2.2. ТЕМА 1. ПОНЯТИЙНЫЙ АППАРАТ В СФЕРЕ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Контрольные вопросы к занятию

5. Основные понятия информационной безопасности и компьютерных преступлений.

6. Компьютерной информация, охраняемая уголовным законом.

7. Понятие компьютерные преступления. Соотношение с категориями преступления в сфере компьютерной информации, киберпреступления, информационные преступления, высокотехнологичные преступления.

8. Проблемы ведения новых терминов и определений: электронные доказательства электронный документ; электронно-цифровые (виртуальные) следы; удаленный (дистанционный) доступ к компьютерной информации; высокотехнологичные способы совершения компьютерных преступлений, транснациональные (трансграничные преступления), кибтерроризм и киберэкстремизм.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Вехов В. Б. Понятие и механизм образования электронно-цифровых следов // Использование современных информационных технологий и проблемы информационной безопасности в деятельности правоохранительных органов: Межвузовский тематический сборник научных трудов. - Калининград: Изд-во Калинингр. ЮИ МВД России, 2009. - С. 62-72.

2. Зверянская, Л.П. Современные проблемы исследования криминалистических особенностей киберпреступлений / Л.П. Зверянская // Приоритетные научные направления: от теории к практике. – 2015.- № 15.- С.127-132.

3. Поляков В.В. К вопросу о противодействии высокотехнологичной транснациональной преступности / В.В. Поляков // Актуальные проблемы отечественной криминалистики: современные тенденции : сборник материалов Международной научно-практической конференции, посвященной памяти Заслуженного юриста РФ, Заслуженного деятеля науки РФ, Заслуженного профессора Московского университета, доктора юридических наук, профессора Николая Павловича Яблокова. - М.: МГУ имени М.В. Ломоносова. Юридический факультет, 2023. – С. 367-374.

4. Поляков В.В. Понятие «высокотехнологичные преступления» в криминалистике // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. 2023. – Т. 28. – № 4. – С. 151 - 188.

5. Поляков, В.В. К вопросу об использовании понятий «виртуальные следы» и «электронно-цифровые следы» в криминалистике / В.В. Поляков, А.В. Шебалин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : матер. одиннадцатой Междунар. науч.-практ. конф. в 2-х частях. – Барнаул : Барнаульский юридический институт МВД России, 2013. – Ч. 1. – С. 123-125.

6. Поляков, В.В. Об использовании новых понятий при доказывании преступлений в сфере компьютерной информации / В.В. Поляков // Российская юридическая наука : состояние, проблемы, перспективы : матер. Всеросс. науч.-практ. конф., посвященной 45-летию юридического образования на Алтае, 19-20 сентября 2008. – Барнаул : Изд-во АлтГУ, 2008. – С 427 - 431.

7. Поляков, В.В. Особенности противодействия кибертерроризму / В.В. Поляков, А.С. Мананников // Информационное противодействие экстремизму и терроризму : Сборник трудов II всероссийской научно-практической конференции (Краснодар, 21 мая 2015 г.) - Краснодар: Краснодарский университет МВД России, 2015. – С. 99-105.

8. Хижняк Д.С. Методологические основы расследования транснациональных преступлений: модельный подход: автореф. дис. д-ра. юрид. наук. - М., 2018.

2.3. ТЕМА 2. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Контрольные вопросы к занятию

1. Соотношение криминалистической, уголовно-правовой, оперативно-розыскной и криминологической характеристик компьютерных преступлений.
2. Понятие криминалистической характеристики компьютерных преступлений. Ее значение и сущность. Проблемы формирования криминалистической характеристики компьютерных преступлений.
3. Предмет и объект компьютерных преступлений.
4. Причины и условия, способствующие совершению преступлений в сфере компьютерной информации.
5. Особенности личности основных участников компьютерных преступлений.
6. Способы и механизмы совершения компьютерных преступлений.
7. Обстановка совершения компьютерных преступлений.
8. Средства совершения компьютерных преступлений.
9. Следовая картина преступлений в сфере компьютерной информации.
10. Корреляционные и причинно-следственные связи элементов криминалистической характеристики компьютерных преступлений.

На проведение занятия отводится 4 часа.

Дополнительная литература

1. Абдусаламов, Р.А. Специфика и способы совершения преступлений в сети Интернет / Р.А Абдусаламов, Ш.Д. Арсланов // Юридический вестник ДГУ. - 2014.- № 1. - С. 116-118.

2. Азиян, В.Г. Исследование проблемы разработки криминалистической характеристики компьютерных преступлений / В.Г. Азизян, Н.И. Журавленко // Евразийский юридический журнал. - 2014. - № 6 (73) - С. 183-187.

3. Беляев, Е.В. Типы личности «компьютерного преступника» / Беляев Е.В. // Вестник Тюменского института повышения квалификации сотрудников МВД России. - 2013. - № 1. - С. 74-77.

4. Бессонов А. А. Объект (предмет) преступного посягательства как элемент криминалистической характеристики преступлений / А. А. Бессонов // Вестник Калмыцкого института гуманитарных исследований РАН. – 2014. - № 4. - С. 231.

5. Богданова, Т.Н. Причины и условия совершения преступлений в сфере компьютерной информации / Т.Н.Богданова // Вестник Челябинского государственного университета.- 2013.-№11.-С.64-67.

6. Будаковский, Д.С. Способы совершения преступлений в сфере компьютерной информации / Д.С. Будаковский // Российский следователь.- 2011. - № 4. - С. 2-4.

7. Введенская, О.Ю. Особенности следообразования при совершении преступлений посредством сети интернет / О.Ю. Введенская // Юридическая наука и правоохранительная практика. - 2015. - № 4 (34). - С. 209-216.

8. Вехов, В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления / В.Б. Вехов // Московский государственный технический университет имени Н.Э. Баумана.-2015.-№8.-С.43-46.

9. Гавло, В.К. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации / В.К. Гавло, В.В. Поляков // Российский юридический журнал. – 2007. – №5 (57). – С. 146-152.

10. Евдокимов, К.Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) / К.Н. Евдокимов // Сибирский юридический вестник. - 2011.- № 1. - С. 86-90.

11. Журкина, О.В. К вопросу о способах совершения мошенничества с использованием сотовой (подвижной) связи / О.В. Журкина, И.В. Бондаренко // Вопросы российского и международного права. - 2015. - № 3-4. - С. 19-30.

12. Лапин, С.А. Программное обеспечение как средство совершения компьютерных преступлений / С.А. Лапин, В.В. Поляков // Ползуновский альманах. - 2016. - №2. – С. 201-204.

13. Лямцев, А.Н. Мобильные коммуникационные устройства и их использование в противоправных целях / А.Н. Лямцев // Вопросы современной науки и практики. Университет им. В.И. Вернадского. - 2014.- № 4 (54).- С. 200-204.

14. Макушев, Д.И. Криминологическая характеристика личности киберпреступника / Д.И. Макушев // Актуальные проблемы гуманитарных и естественных наук.- 2016.- № 1-3. - С. 202-204.

15. Малышкин, П.В. Способы сокрытия преступлений, совершаемых с применением информационных компьютерных технологий / П.В. Малышкин // Вестник Мордовского университета. - 2014. Т. 24. - № 4. - С. 42-47.

16. Маслакова, Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика /Е.А. Маслакова // Политика и право. -2014. -№ 1.- С. 114-121.

17. Морар, И.О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? / И.О. Морар // Российский следователь.- 2012.- № 13.-С.34-38.

18. Мочагин, П.В. Виртуально-информационный и невербальный процесс отражения следообразований как новое направление в

криминалистике и судебной экспертизе /П.В. Мочагин // Вестник Удмуртского университета.-2013.-№ 2.- С.148-154.

19. Поляков, В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации / В.В. Поляков, С.М. Слободян // Известия Томского политехнического университета. – 2007. – Т. 310, № 1. – С. 212 – 216.

20. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия Алтайского государственного университета.-2013.- Выпуск № 2 (78) / том 1.-С.114-115.

21. Поляков, В.В. Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации / В.В. Поляков // Региональные аспекты технической и правовой защиты информации : монография / В.В. Поляков, В.А. Трушев, И.А. Рева и др. – Барнаул : Изд-во Алт. ун-та, 2013. – Гл. 1. – С. 9-42.

22. Поляков, В.В. Средства совершения компьютерных преступлений / В.В. Поляков, С.А. Лапин // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2014. - № 2 (32). - С. 162-166.

23. Рогозин, В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий / В.Ю. Рогозин // Расследование преступлений: проблемы и пути их решения.-2015.- № 1 (7).- С. 56-58.

24. Смагоринский, Б.П. О способах совершения мошенничеств с использованием сотовой связи Б.П. Смагоринский, М.С. Дьяконов, М.С. Дронова // Вестник Волгоградской академии МВД России.- 2014.- № 2 (29). - С. 98-104.

25. Тулегенов, В.В. Киберпреступность как форма выражения криминального профессионализма / В.В. Тулегенов // Криминология: вчера, сегодня, завтра. – 2014.- №2(33).- С.94-97.

2.4. ТЕМА 3. ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию

1. Общие положения организации работы по выявлению и расследованию компьютерных преступлений.
2. Выдвижение следственных версий.
3. Планирование расследования.
4. Создание следственной группы и налаживание взаимодействия в ней.
5. Помощь специалистов в подготовке к следственным действиям.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Вехов, В.Б Теоретические и прикладные проблемы применения программного обеспечения специального назначения при расследовании преступлений в сфере компьютерной информации / В.Б. Вехов, С.А. Ковалев // Вестник Воронежского института МВД России. - 2012. - №1
2. Вехов, В.Б. Возможности правоохранительных органов по противодействию ddos-атакам // Защита информации. Инсайд. - 2008. - № 3. - С. 77-82.
3. Данилова, Р.Р. Разрешение типичных задач допроса по компьютерным преступлениям / Р.Р. Данилова, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск III / Сборник научных статей. - Барнаул: Изд-во Алт. ун-та, 2015. – С. 132-135.
4. Ковалев, С.А Некоторые аспекты моделирования при расследовании преступлений в сфере компьютерной информации С.А. Ковалев // Бизнес в законе Экономико-юридический журнал. - 2009. - № 1

5. Косынкин, А.А. Оперативно-розыскное сопровождение расследования преступлений в сфере компьютерной информации / А.А. Косынкин // Библиотека криминалиста. – 2013. - №5. - С. 103-115.

6. Лядских, В.В Преступления в сфере компьютерной информации В.В. Лядских // Электронный вестник Ростовского социально-экономического института. - 2014. - № 2

7. Нарижный А.В. Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий // «Черные дыры» в российском законодательстве. - 2012. - № 5. – 38 с.

8. Никитин, А.С. Некоторые вопросы, связанные с изъятием компьютерной информации в рамках доследственной проверки / А.С. Никитин, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Изд-во Новый формат, 2016. – С. 254-259.

9. Подольный, Н.А. Некоторые особенности выявления, раскрытия и расследования компьютерных преступлений/ Н.А. Подольный // Российский следователь. - 2014. - № 1. - С. 11

10. Поляков В.В. Анализ факторов, затрудняющих расследование неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации: сб. научн. ст. - Барнаул: Изд-во Алт. ун-та, 2008. - С. 17 - 24.

11. Поляков, В.В. Некоторые проблемы раскрытия преступлений в сфере компьютерной информации / В.В. Поляков, А.А. Макогон // Проблемы правовой и технической защиты информации. Выпуск V / Сборник научных статей. - Барнаул: Изд-во Алт. ун-та, 2017. – С. 85-88.

12. Поляков, В.В. Некоторые сложности расследования компьютерных преступлений / В.В. Поляков, С.А. Лапин // Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях : матер. Междунар. научн.-практ. конф. (Тюмень, 1-2 ноября 2013 г.). – Тюмень, 2013. – Вып. 10, Ч. 2. – С. 208-

211.

13. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 96-101 с.

14. Поляков, В.В. Противодействие распространению наркотических средств в интернет-пространстве / В.В. Поляков // Антинаркотическая безопасность. – 2015. – № 1 (4) - С. 68-70.

15. Поляков, В.В. Этапы осмотра места происшествия по компьютерным преступлениям / В.В. Поляков // Закон и право. - 2016. - № 11. - С. 112-114.

16. Рогачкина, Е.А. Понятие, функции и значение способа совершения преступления// Северо-Кавказский юридический вестник, 2011, №1. С 81-85.

17. Сарапулов А.А. Теоретико-прикладные проблемы доказательств о преступлениях в сфере компьютерной информации // Правовые вопросы связи. - 2011. - N 1. - С. 8.

18. Шаевич А.А. Особенности организации взаимодействия со сведущими лицами в области компьютерных технологий при раскрытии и расследовании преступлений // Известия Иркутской государственной экономической академии. 2013. № 5. – С. 74 – 76.

2.5. ТЕМА 4. СЛЕДСТВЕННЫЕ СИТУАЦИИ И ИХ РАЗРЕШЕНИЕ В ХОДЕ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

Контрольные вопросы к занятию

1. Ситуационный подход в криминалистике.
2. Структура криминалистических ситуаций.
3. Понятия криминальная ситуация, следственная ситуация, криминалистическая ситуация. Их соотношение.
4. Виды следственных ситуаций, возникающих при расследовании компьютерных преступлений.
5. Типизация криминалистических ситуаций.
6. Алгоритмы разрешения следственных ситуаций.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Гавло, В.К. Ситуационный подход в криминалистике по делам о компьютерных преступлениях / В.К. Гавло, В.В. Поляков // Научно-методические и нормативные материалы и документы IV Пленума СибРОУМО по образованию в области информационной безопасности : матер. Пленума и документы конференции : сб. статей : Томск – Барнаул – Белокуриха, 8-13 июня 2010 г. – Томск : «В-Спектр», 2010. – С. 186 - 187.
2. Иванченко Р.Б. Необходимость разработки следственных ситуаций и тактических операций при расследовании неправомерного доступа к компьютерной информации // Вестник Саратовской государственной юридической академии. 2014. № 5 (51). С. 124.
3. Косынкин А.А. Соотношение конфликта и противодействия при расследовании преступлений в сфере компьютерной информации Российский следователь. 2011. N 10. С. 28 - 29.
4. Криминалистика: учебник Яблоков Н.П. М.: Юрайт, 2011.

5. Поляков, В.В. Анализ судебной практики Алтайского края по преступлениям в сфере компьютерной информации / В.В. Поляков // Вестник Новосибирского государственного университета. Серия: Право. - 2014. - Т. 10. - № 1. - С. 99-103.

6. Поляков, В.В. К вопросу о типичных следственных ситуациях первоначального этапа расследования незаконного сбыта курительных смесей / В.В. Поляков, А.В. Шебалин // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: матер. двенадцатой Междунар. науч.-практ. конф. – Барнаул: Барнаульский юридический институт МВД России, 2014. – С. 123-125.

7. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 96-101 с.

8. Поляков, В.В. Особенности производства осмотра по компьютерным преступлениям / В.В. Поляков // Российский следователь. - 2017. - № 21. - С. 14-17.

9. Поляков, В.В. Проблемы производства судебных компьютерно-технических экспертиз / В.В. Поляков, С.И. Маюнов // Евразийский юридический журнал. - 2016. - № 10 (101). – С. 233-235.

10. Поляков, В.В. Проблемы тактики допроса по делам о компьютерных преступлениях / В.В. Поляков, А.В. Ширяев // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: матер. тринадцатой Междунар. науч.-практ. конф.: в 3 ч. – Барнаул: Барнаульский юридический институт МВД России, 2015. – Ч. 1.– С. 123-126.

11. Поляков, В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации / В.В. Поляков // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – N1(21). – С. 46 - 50.

12. Поляков, В.В. Этапы осмотра места происшествия по компьютерным преступлениям / В.В. Поляков // Закон и право. - 2016. - № 11. - С. 112-114.

13. Шагидаев М.С. Алгоритм действий следователя в типичных следственных ситуациях первоначального этапа расследования компьютерных преступлений // Евразийский юридический журнал. 2011 - №7 (38). С. 96-98.

2.6. ТЕМА 5. ОСОБЕННОСТИ ОСМОТРА ПО КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Контрольные вопросы к занятию

1. Понятие и содержание осмотра места происшествия.
2. Задачи и вопросы, разрешаемые при его проведении.
3. Этапы осмотра места происшествия.
4. Научно-технические средства, применение при осмотре места происшествия по делам о компьютерных преступлениях.
5. Тактические приемы осмотра.
6. Негативные обстоятельства, устанавливаемые при осмотре места происшествия.
7. Фиксация хода и результатов осмотра места происшествия.
8. Правила изъятия и хранения предметов и следов, изъятых в ходе осмотра места происшествия.
9. Особенности осмотра средств компьютерной техники.
10. Содержание и задачи.
11. Вопросы, разрешаемые при его проведении.
12. Особенности участия специалиста при производстве данного следственного действия.
13. Подготовка к проведению осмотра средств компьютерной техники.
14. Применение научно-технических средств и методов при производстве осмотра.
15. Этапы осмотра средств компьютерной техники.

На проведение занятия отводится 4 часа.

Дополнительная литература

1. Криминалистика: учебник под общ. ред. А. Г. Филиппова М.: Юрайт, 2011

2. Мусаева У.А. Специфика проведения следственного осмотра по делам о преступлениях в сфере компьютерной информации / У.А. Мусаева // Известия Тульского государственного университета. Экономические и юридические науки.- 2013 г. Выпуск № 4-2.

3. Никитин, А.С. Некоторые вопросы, связанные с изъятием компьютерной информации в рамках доследственной проверки / А.С. Никитин, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Изд-во Новый формат, 2016. – С. 254-259.

4. Никулина, О.А. Особенности тактики производства осмотра места происшествия по делам о преступлениях в сфере компьютерной информации / О.А. Никулина // Вестник Воронежского института ФСИН России.- 2015.- № 2. С. 68-71.

5. Оконенко, Р.И. К вопросу о правомерности осмотра компьютера как следственного действия / Р.И. Оконенко // Адвокат. – 2015 г. - № 1. - С. 27-30.

6. Поляков, В.В. Анализ судебной практики Алтайского края по преступлениям в сфере компьютерной информации / В.В. Поляков // Вестник Новосибирского государственного университета. Серия: Право. - 2014. - Т. 10. - № 1. - С. 99-103.

7. Поляков, В.В. Некоторые проблемы раскрытия преступлений в сфере компьютерной информации / В.В. Поляков, А.А. Макогон // Проблемы правовой и технической защиты информации. Выпуск V / Сборник научных статей. - Барнаул: Изд-во Алт. ун-та, 2017. – С. 85-88.

8. Поляков, В.В. Некоторые сложности расследования компьютерных преступлений / В.В. Поляков, С.А. Лапин // Совершенствование деятельности правоохранительных органов по борьбе с

преступностью в современных условиях : матер. Междунар. научн.-практ. конф. (Тюмень, 1-2 ноября 2013 г.). – Тюмень, 2013. – Вып. 10, Ч. 2. – С. 208-211.

9. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. I. Организационные основы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV. - С. 87-95.

10. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 96-101 с.

11. Поляков, В.В. Особенности производства осмотра по компьютерным преступлениям / В.В. Поляков // Российский следователь. - 2017. - № 21. - С. 14-17.

12. Поляков, В.В. Этапы осмотра места происшествия по компьютерным преступлениям / В.В. Поляков // Закон и право. - 2016. - № 11. - С. 112-114.

13. Романенко, М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения / М.А. Романенко // Вестник Омского университета. Серия «Право». – 2008 г.- № 1 (14). С. 171–175.

14. Скоромников, К. С. Осмотр места происшествия по делам о преступлениях в сфере компьютерной информации / К. С. Скоромников // Осмотр места происшествия : практич. пособие. – М., 2000. – С. 25.

15. Ширяев, А.В. Некоторые приемы производства осмотра по преступлениям в сфере компьютерной информации / А.В. Ширяев, В.В. Поляков // Труды молодых ученых Алтайского государственного университета: материалы 43-й научной конференции студентов, магистрантов, аспирантов и учащихся лицейных классов. - Вып. 13. - Барнаул: Изд-во Алт. ун-та, 2016. 592 с.

2.7. ТЕМА 6. ПРОИЗВОДСТВО ОБЫСКА И ВЫЕМКИ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Контрольные вопросы к занятию

1. Понятие, сущность и задачи обыска и выемки по делам о компьютерных преступлениях.
2. Применение научно-технических средств, используемых в ходе обыска и выемки по компьютерным преступлениям.
3. Тактика обыска в помещении.
4. Фиксация хода и результатов обыска протоколом.

На проведение занятия отводится 2 часов.

Дополнительная литература

1. Илюшин, Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг «Интернет»/ Д.А. Илюшин //Вестник Муниципального института права и экономики (МИПЭ). Вып. 1. – Липецк: Изд-во НОУ «Интерлингва», 2013. - С. 77.
2. Краснова, Л. Б. "Обыск-осмотр" средств компьютерной техники / Л. Б. Краснова // Воронежские криминалистические чтения. – Воронеж, 2000. – Вып. 1. – С. 106.
3. Никитин, А.С. Некоторые вопросы, связанные с изъятием компьютерной информации в рамках доследственной проверки / А.С. Никитин, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Изд-во Новый формат, 2016. – С. 254-259.
4. Поляков, В.В. Анализ судебной практики Алтайского края по преступлениям в сфере компьютерной информации / В.В. Поляков // Вестник Новосибирского государственного университета. Серия: Право. - 2014. - Т.

10. - № 1. - С. 99-103.

5. Поляков, В.В. Некоторые проблемы раскрытия преступлений в сфере компьютерной информации / В.В. Поляков, А.А. Макогон // Проблемы правовой и технической защиты информации. Выпуск V / Сборник научных статей. - Барнаул: Изд-во Алт. ун-та, 2017. – С. 85-88.

6. Поляков, В.В. Некоторые сложности расследования компьютерных преступлений / В.В. Поляков, С.А. Лапин // Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях : матер. Междунар. научн.-практ. конф. (Тюмень, 1-2 ноября 2013 г.). – Тюмень, 2013. – Вып. 10, Ч. 2. – С. 208-211.

7. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. I. Организационные основы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 87-95.

8. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. II. Теоретические и практические проблемы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 96-101.

9. Поляков В.В. Особенности производства осмотра по компьютерным преступлениям / В.В. Поляков // Российский следователь. - 2017. - № 21. - С. 14-17.

10. Поляков В.В. Этапы осмотра места происшествия по

компьютерным преступлениям / В.В. Поляков // Закон и право. - 2016. - № 11. - С. 112-114.

11. Пропастин С.В Осмотр, обыск или судебная экспертиза: проблема выбора при расследовании преступлений, совершаемых с использованием интернет-технологий / С.В. Пропастин // Научный вестник Омской академии МВД России. -2015. - № 2 (57), С. 20-23.

12. Сарапулов А.А. Теоретико-прикладные проблемы доказательств о преступлениях в сфере компьютерной информации Правовые вопросы связи. 2011. N 1. С. 8.

2.8. ТЕМА 7. ДОПРОС ПОДОЗРЕВАЕМЫХ, ОБВИНЯЕМЫХ И СВИДЕТЕЛЕЙ ПО ДЕЛАМ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ

Контрольные вопросы к занятию

1. Понятие, сущность, задачи и значение допроса по делам о компьютерных преступлениях.
2. Подготовка к допросу.
3. Организация вызова на допрос.
4. Составление плана проведения следственного действия.
5. Классификация тактических приемов допроса.
6. Тактические приемы допроса подозреваемых, потерпевших, свидетелей, специалистов и экспертов.
7. Фиксация хода и результатов допроса.

На проведение занятия отводится 2 часов.

Дополнительная литература

1. Данилова, Р.Р. Разрешение типичных задач допроса по компьютерным преступлениям / Р.Р. Данилова, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск III / Сборник научных статей. - Барнаул: Изд-во Алт. ун-та, 2015. – С. 132-135.
2. Марданов, А.Б. Некоторые аспекты допроса в отношении лиц, совершивших преступления в сфере компьютерной информации/ А.Б. Марданов // Российский следователь. - 2014. - № 23. - С. 30
3. Поляков, В.В. Проблемы тактики допроса по делам о компьютерных преступлениях / В.В. Поляков, А.В. Ширяев // Актуальные проблемы борьбы с преступлениями и иными правонарушениями: матер. тринадцатой Междунар. науч.-практ. конф.: в 3 ч. – Барнаул: Барнаульский юридический институт МВД России, 2015. – Ч. 1.– С. 123-126.

4. Салтевский, М.В. Проблемы противодействия преступности в сфере компьютерных технологий / М.В. Салтаевский. - М.: Юркнига, 2010. – 378 с.

2.9. ТЕМА 8. ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ПОЗНАНИЙ. СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА

Контрольные вопросы к занятию

1. Помощь специалистов и экспертов по делам о компьютерных преступлениях.
2. Соотношение компьютерной и судебной компьютерно-технической экспертизы.
3. Понятие и содержание судебной компьютерно-технической экспертизы.
4. Назначение судебной компьютерно-технической экспертизы.
5. Особенности экспертизы компьютеров, их отдельных устройств и комплектующих.
6. Особенности экспертизы компьютерных данных и программного обеспечения.
7. Особенности сетевых компьютерно-технических экспертиз.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Быков, С.Ю. Некоторые сложности производства судебных компьютерно-технических экспертиз / С.Ю. Быков, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Изд-во Новый формат, 2016. – С. 166-172.
2. Егорышева Е.А., Егорышев А.С. Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации // Эксперт-криминалист. 2012. № 3. - С. 14 - 16.
3. Кукарникова, Т. Э. Проблема криминалистического исследования электронных документов / Т. Э. Кукарникова // Известия ТулГУ. Серия,

"Современные проблемы законодательства России, юридических наук и правоохранительной деятельности". – 2000. – Вып. 3. – С. 141.

4. Куликова, О.Н Вопросы и типичные ошибки, допускаемые следователями при назначении судебной компьютерной экспертизы / О.Н. Куликова., С.Ю. Скобелин // Расследование преступлений: проблемы и пути их решения. - 2015. - № 1 (7). -С. 135-137.

5. Малышкин, П.В. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий, связанные с оказываемым ему противодействием / П.В. Малышкин // Библиотека криминалиста. – 2013. - №5, С. 245-255

6. Мешков, В.М., Григорьев А.Н. Некоторые аспекты формирования научных основ расследования преступлений, сопряженных с использованием средств компьютерной техники / В.М. Мешков., А.Н. Григорьев // Библиотека криминалиста. -2013. - №5, С. 256-264

7. Моргуненко, А.В Автоматизированный комплекс для экспертизы жесткого диска компьютера А.В. Моргуненко., Д.С. Никифоров., И.Ю. Поляков., А.К. Пономарев // Электронные средства и системы управления. - 2013. - № 2, С. 27-28.

8. Поляков, В.В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации / В.В. Поляков, А.В. Шебалин // Сборник материалов криминалистических чтений / под ред. Ю.Л. Бойко. – Барнаул : Барнаульский юридический институт МВД России, 2013. – С. 73-75.

9. Поляков, В.В. Проблемы производства судебных компьютерно-технических экспертиз / В.В. Поляков, С.И. Маюнов // Евразийский юридический журнал. - 2016. - № 10 (101). – С. 233-235. ISSN 2073-4506 1812-3783

10. Поляков, В.В. Судебная компьютерно-техническая экспертиза средств мобильной радиосвязи / В.В. Поляков // Известия Алтайского государственного университета. – 2014. – № 2/2. – С. 140-143.

11. Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: Автореф. дис. ... д-ра юрид. наук. - М., 2002. – 54 с.

12. Шаевич А.А. Особенности организации взаимодействия со сведущими лицами в области компьютерных технологий при раскрытии и расследовании преступлений // Известия Иркутской государственной экономической академии. 2013. № 5. – С. 74 – 76.

2.10. ТЕМА 9. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

Контрольные вопросы к занятию

5. Понятие, сущность, задачи и значение проверки показаний на месте происшествия. Особенности подготовки и проведения данных следственных действий. Тактические приемы, применяемые при их производстве.

6. Понятие, сущность, задачи и значение следственного эксперимента. Особенности подготовки и проведения данных следственных действий. Тактические приемы, применяемые при их производстве.

7. Понятие, сущность, задачи и значение опознания. Особенности подготовки и проведения данных следственных действий. Тактические приемы, применяемые при их производстве.

8. Понятие, сущность, задачи и значение контроля и записи переговоров, получения информации о соединениях между абонентами и (или) абонентскими устройствами по делам о компьютерных преступлениях. Особенности подготовки и проведения данных следственных действий. Тактические приемы, применяемые при их производстве.

9. Особенности производства иных следственных действий.

На проведение занятия отводится 2 часа.

Дополнительная литература

1. Махтаев М.Ш. Методика расследования компьютерных преступлений. - М.: Юристъ, 2017. – 531 с.

2. Сарапулов А.А. Теоретико-прикладные проблемы доказательств о преступлениях в сфере компьютерной информации // Правовые вопросы связи. - 2011. - N 1. - С. 8.

3. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. - Воронеж: Издательство Воронежского государственного университета, 2002. – 437 с.

4. Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. - 2010. - № 2. - С. 121-126.

5. Следственные действия: учебник / Савельева М.В. М.: Юрайт, 2011.

2.11. ПРИМЕРНЫЕ ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Понятие, сущность и виды компьютерных преступлений.
2. Понятие, сущность и значение криминалистической характеристики преступлений в сфере компьютерной информации.
3. Элементы криминалистической характеристики преступлений в сфере компьютерной информации.
4. Способ совершения компьютерных преступлений.
5. Обстановка совершения компьютерных преступлений.
6. Личность преступника.
7. Следовая картина преступлений в сфере компьютерной информации.
8. Причины и условия, способствующие совершению преступлений в сфере компьютерной информации.
9. Обстоятельства, препятствующие расследованию компьютерных преступлений.
10. Понятие и содержание обстоятельств, подлежащих установлению по делам о преступлениях в сфере компьютерной информации и высоких технологий.
11. Поводы и основания для возбуждения уголовного дела по компьютерному преступлению.
12. Организация и особенности проведения предварительной проверки заявлений и сообщений о преступлении в сфере компьютерной информации.
13. Понятие и содержание осмотра места происшествия, проводимого по делам о преступлениях, совершенных в сфере компьютерной информации.
14. Подготовка к осмотру места происшествия по делам о преступлениях, совершенных в сфере компьютерной информации и высоких технологий.

15. Этапы осмотра места происшествия и тактические приемы его проведения.

16. Организация работы следственной группы при осмотре места происшествия.

17. Организация взаимодействия следователя, оперативных сотрудников и сотрудников других служб ОВД по раскрытию и расследованию преступлений в сфере компьютерной информации

18. Фиксация хода и результатов осмотра места происшествия по делам о компьютерных преступлениях. Правила изъятия и хранения предметов и следов, изъятых в ходе осмотра места происшествия.

19. Научно-технические средства, используемые в ходе осмотра места происшествия по делам о компьютерных преступлениях.

20. Следственные версии и планирование расследования по делам о преступлениях в сфере компьютерной информации.

21. Следственные ситуации и их разрешение в ходе предварительного расследования компьютерных преступлений.

22. Судебные ситуации и их разрешение по компьютерным преступлениям.

23. Содержание, задачи и порядок осмотра средств компьютерной техники. Оформление хода и результатов следственного действия.

24. Тактика допроса подозреваемого в компьютерном преступлении.

25. Тактика допроса обвиняемого в совершении компьютерного преступления.

26. Тактика допроса потерпевших и свидетелей по делам о компьютерных преступлениях.

27. Использование специальных познаний при производстве расследования преступлений, совершенных в сфере компьютерной информации.

28. Понятие и содержание судебной компьютерно-технической экспертизы.

29. Содержание и структура криминалистического предупреждения компьютерных преступлений.

30. Меры обеспечения криминалистического предупреждения компьютерных преступлений.

2.12. ТЕМЫ РЕФЕРАТОВ И НАУЧНЫХ ДОКЛАДОВ

1. Способы совершения компьютерных преступлений.
2. Обстановка совершения компьютерных преступлений.
3. Особенности следовой картины компьютерных преступлений.
4. Причины и условия, способствующие совершению преступлений в сфере компьютерной информации.
5. Обстоятельства, препятствующие расследованию компьютерных преступлений.
6. Понятие и содержание обстоятельств, подлежащих установлению и доказыванию по делам о преступлениях в сфере компьютерной информации.
7. Особенности поводов и оснований для возбуждения уголовного дела по компьютерному преступлению.
8. Организация и особенности проведения предварительной проверки заявлений и сообщений о преступлении в сфере компьютерной информации.
9. Этапы осмотра места происшествия и тактические приемы его проведения.
10. Организация взаимодействия следователя, оперативных сотрудников и специалистов по расследованию преступлений в сфере компьютерной информации
11. Научно-технические средства, используемые в ходе расследования компьютерных преступлениях.
12. Следственные версии и планирование расследования по делам о преступлениях в сфере компьютерной информации.
13. Судебно-следственные ситуации по компьютерным преступлениям
14. Тактика допроса подозреваемого, обвиняемого, потерпевшего и свидетеля в компьютерном преступлении.

15. Использование специальных познаний при производстве расследования преступлений, совершенных в сфере компьютерной информации.

16. Доказывание и доказательства преступлений в сфере компьютерной информации.

17. Определение ущерба, причиненного преступлением в сфере компьютерной информации.

ГЛАВА 3. ПРЕДУПРЕЖДЕНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

3.1. Теоретические положения криминалистического предупреждения компьютерных преступлений

Предупреждение преступлений является одним из наиболее эффективных путей борьбы с преступностью. Предупреждение преступлений представляет собой весьма сложный и многоплановый комплекс мер различного характера. Одной из основных частей этого комплекса является криминалистическое предупреждение преступлений.

Согласно М.Ш. Махтаеву, криминалистическое предупреждение преступлений - это система знаний о «закономерностях возникновения, обнаружения, собирания, исследования, оценки и использования криминалистически значимой информации об обстоятельствах, способствующих совершению и сокрытию преступлений», а также о «специальных средствах, приемах и методах криминалистики, направленных на предупреждение готовящихся и пресечение начавшихся преступлений»[38].

Субъектами предупреждения являются, во-первых, следователи и дознаватели; во-вторых, эксперты; в-третьих, сотрудники прокуратуры; в-четвертых, судьи.

Неразработанность теории криминалистического предупреждения наиболее заметна для противодействия новым видам преступности, например, связанным с привлечением высоких технологий. Прежде всего, это относится к высокотехнологичным преступлениям[39].

За последние годы существенно изменилась картина преступлений в

[38] Махтаев, М.Ш. Основы теории криминалистического предупреждения преступлений / М.Ш. Махтаев. - М.: Изд-во «Раритет», 2001. - С. 96.

[39] Поляков, В.В. Перспективы переподготовки и повышения квалификации сотрудников правоохранительных органов / В.В. Поляков, В.А. Мазуров, А.А. Исаев, Т.В. Сидоренко // Алтай-Азия 2014: Евразийское образовательное пространство - новые вызовы и лучшие практики: матер II Международного образовательного форума (Барнаул, 25–26 сентября 2014 г.). – Барнаул: Изд-во Алт. ун-та, 2014. – С. 82-85.

сфере компьютерной информации. Это связано с тем, что общество стало более остро на них реагировать. Реальность привлечения к уголовной ответственности привела к более продуманному способу совершения, а также сокрытию преступлений. Распространенные ранее простые виды преступлений, сейчас становятся редкостью. Им на смену пришли высокотехнологичные способы совершения преступлений, в которых в первую очередь присутствует подготовка и сокрытие преступления, а также противодействие расследованию, применяются новые или модифицированные средства и используются дистанционные технологии[40]. В результате становится наиболее велика латентность таких преступлений[41].

Особую значимость для развития теории и для нужд практики имеет построение системы классификации мер по обеспечению криминалистического предупреждения преступлений. Такая классификация по своей структуре должна быть аналогична общей классификации мер профилактической деятельности, обладая при этом существенной собственной спецификой. При анализе мер профилактики преступлений в сфере компьютерной информации высказывались разные точки зрения на систему соответствующих действий. Так, А.С. Белоусов выделяет три направления профилактических мер: правовое; организационно-техническое и криминалистическое[42]. В. Федоров пишет о двух направлениях профилактической работы - организационно-техническом и правовом[43]. Э. Мелик выделяет три группы мер: правовые, организационно-технические и

[40] Поляков, В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации / В.В. Поляков // Доклады Томского государственного университета. – 2010. – N1 (21). – С. 46 - 50.

[41] Поляков В.В. Латентность высокотехнологичных преступлений: понятие, структура, методы оценки уровня / В.В. Поляков // Всероссийский криминологический журнал. – 2023. – Т. 17, № 2. – С. 146–155.

[42] Белоусов, А.С. Некоторые аспекты расследования компьютерных преступлений / А.С. Белоусов // Информационные технологии и безопасность: сб. науч. тр. Междунар. конф. – Киев: Национальная академия наук Украины, 2003. – Вып. 3. – С. 20.

[43] Федоров, В. Компьютерные преступления: выявление, расследование и профилактика / В. Федоров // Законность. - 1994. - № 6. - С. 44 – 47.

криминалистические[44].

Структура мер обеспечения в случае криминалистического предупреждения преступлений исследована достаточно поверхностно. Относительно проработанная система предложена в работе М.Ш. Махтаева, подразделяющего эти меры на следующие три группы: правовое обеспечение; организационное обеспечение; информационное обеспечение. Такая классификация является не полной, т.е. не включает в себя все основные элементы. Это особенно заметно в случае высокотехнологичных преступлений, для которых необходимо выделить в отдельную группу технические меры. Именно, обнаружение и предотвращение готовящихся преступлений, их раскрытие и расследование невозможно без использования арсенала специальных технических средств, включающих в себя средства компьютерной техники, специальное оборудование и программное обеспечение, методики по их применению.

Система мер криминалистического предупреждения. Все меры предупреждения компьютерных преступлений наиболее правильно объединить в следующие четыре группы:

- меры правового обеспечения;
- меры организационного обеспечения;
- меры технического обеспечения;
- меры методического обеспечения[45].

Многие из мер криминалистического предупреждения преступлений имеют комплексный характер и реально могут быть реализованы только при сочетании нескольких из указанных направлений (например, организационных и технических мер).

---

[44] Мелик, Э. Компьютерные преступления (информационно-аналитический обзор) [Электронный ресурс] / Э. Мелик. – Электрон. дан. - Режим доступа: http://www.melik.narod.ru, свободный.

[45] Поляков, В.В. Особенности профилактики преступлений в сфере неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации: сб. научн. ст. - Барнаул: Изд-во Алт. ун-та, 2008. - С. 15.

Меры правового обеспечения.

К правовым мерам предупреждения компьютерных преступлений, прежде всего, нужно отнести разработку и принятие новых, изменение и совершенствование существующих норм законодательства, устанавливающих ответственность за эти деяния. Однако сюда же входят также конкретные меры правоприменения.

Нельзя не остановиться на точке зрения, отстаиваемой в последнее время рядом как ученых-криминалистов, так и практиков и заключающейся в необходимости усилить наказания за компьютерные преступления[46]. Полагаем, что это совершенно справедливо для отличающихся повышенной общественной опасностью высокотехнологичных преступлений. Анализ экспертных мнений показывает, что подобной точки зрения придерживается значительная часть сотрудников правоохранительных органов Алтайского края.

Со стороны сотрудников правоохранительных органов неоднократно высказывалось пожелание создания группы «дежурных специалистов», имеющих знания в области информационных технологий[47]. Объясняется это значительными трудностями обеспечения участия в следственных действиях при изъятии компьютерной информации таких специалистов. Привлечение специалистов в конкретных узких областях знаний, особенно в условиях периферийных районов, может быть затруднительно и сопряжено с существенными материально-финансовыми затратами. Решение данных проблем занимает много времени, в ходе которого обстановка места происшествия может критически измениться и могут быть утрачена

[46] Погодин, С.Б. Особенности расследования преступлений в сфере компьютерной информации / С.Б. Погодин // Российский следователь. - 2004. - № 7. - С. 6 – 9.

[47] Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. I. Организационные основы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV. - С. 87-95.

возможность получения следов-последствий преступления. В связи с этим принятие правовых актов, направленных на создание группы штатных (или на общественных началах внештатных) «дежурных специалистов» для оперативного привлечения их в состав следственной группы улучшило бы противодействие компьютерной преступности.

Подчеркнем, что в ходе расследования следователь имеет право применять ряд предупредительных мер, именно, он может вносить представление (статья 158 УПК РФ). Такие представления являются процессуальными документами и вносятся в государственный орган или в организацию, а также должностному лицу. Предупредительные меры могут содержаться в этих представлениях в качестве рекомендаций (например, по устранению конкретных последствий преступления или причин, способствующих совершению преступлений). Следственная практика показывает, что уже на стадии возбуждения уголовного дела у следователя может быть достаточно информации для того, чтобы он мог внести представление, предупреждающее повторение преступления. Следователь может предупреждать совершение преступлений также иными своими действиями, например, изымая средства совершения преступлений в ходе осмотра места происшествия.

В эту же группу мер входят международные нормативные акты, регулирующие взаимодействие между правоохранительными органами различных стран. Требуется взаимное признание соответствующих следственных документов, заключение межгосударственных договоров о сотрудничестве в данной области и т.д.[48] Как указывает S. County, должны быть введены специальные правила, которые могли бы развиваться в международном сообществе и благодаря которым был бы дозволен прямой

[48] Стригалев Б.Р. Вопросы методики и тактики расследования уголовных дел о преступлениях, связанных с использованием компьютерной техники [Электронный ресурс]: Компьютеры в уголовном судопроизводстве: матер. криминалистического семинара 31 марта 1997 г. / Б.Р. Стригалев. - Электрон. дан. - СПб.: Санкт-Петербургский юридический институт Генеральной прокуратуры РФ, 1998. - Режим доступа: http://nadzor.pk.ru/analit/show_a.php?id=540.

доступ к иностранным базам данных посредством телекоммуникационных систем, а длительные процедуры взаимных разрешений и содействий просто аннулированы[49]. В рамках действующего международного законодательства он полагает возможным применение двух мер, которые можно использовать, чтобы добиться взаимодействия участвующих в расследовании правоохранительных органов различных государств: обязанность отдавать для изъятия или выемки искомые доказательства и обязанность давать свидетельские показания. В процессе взаимодействия между правоохранительными органами различных стран появляется возможность привлечения ведущих специалистов по защите информации к предупреждению преступлений[50].

Меры организационного обеспечения.

При анализе данной группы мер представляется полезным выделить два основных направления: меры, направленные на совершенствование работы правоохранительных органов, и меры, относящиеся к организации деятельности конкретных организаций, предприятий, физических лиц.

Правильным является создание специализированных подразделений по борьбе с преступлениями в сфере высоких технологий и создание следственных групп, специализирующихся на таких преступлениях, а также поручение расследования следователям, имеющим положительный опыт в таких делах. Таким сотрудникам легче осуществлять работу по криминалистическому предупреждению компьютерных преступлений.

Важное значение имеет организация взаимодействия различных

[49] County S. Computer Crime [Электронный ресурс] / S. County. – Электрон. дан. - Режим доступа: http://www.mobrien.com, свободный.

[50] Стригалев Б.Р. Вопросы методики и тактики расследования уголовных дел о преступлениях, связанных с использованием компьютерной техники [Электронный ресурс]: Компьютеры в уголовном судопроизводстве: матер. криминалистического семинара 31 марта 1997 г. / Б.Р. Стригалев. - Электрон. дан. - СПб.: Санкт-Петербургский юридический институт Генеральной прокуратуры РФ, 1998. - Режим доступа: http://nadzor.pk.ru/analit/show_a.php?id=540.

правоохранительных органов, в том числе различных регионов[51].

Важным направлением криминалистического предупреждения преступлений представляется усиление прокурорского надзора, поскольку «именно прокурор обладает властно-распорядительными полномочиями. Важность и своевременность этой меры в немалой степени связана с частым отказом в возбуждении уголовных дел по компьютерным преступлениям и необоснованным их прекращением.

Отдельной не терпящей отлагательства задачей является организация действенной системы подготовки и переподготовки кадров для соответствующих подразделений правоохранительных органов с упором на получение компетенций в области криминалистического предупреждения компьютерных преступлений.

Организационные меры криминалистического предупреждения по отношению к организациям можно подразделить на внутренние и внешние. Внутренние меры направлены на предотвращение преступлений со стороны персонала. Внешние – направлены на профилактику совершения преступлений со стороны иных лиц, прежде всего, использующих в качестве средства совершения преступлений информационно-коммуникационные сети.

Организационные меры криминалистического предупреждения должны быть направлены на комплексное обеспечение информационной безопасности. Так, Л.И. Аркуша справедливо пишет: «Охрану компьютерных систем, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра,

[51] Пак, П.Н. Некоторые аспекты прокурорского надзора за расследованием преступлений в сфере компьютерной информации [Электронный ресурс] / П.Н. Пак. – Электрон. дан. - Режим доступа: http://pravgos.narod.ru/html/library/yang_sience/ys_lib_pak_001.htm, свободный.

универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.»[52]. Необходим осуществлять тщательный подбор сотрудников, проведение регулярных проверок и инструктажей, возложение ответственности за информационную безопасность на специально обученных лиц. Целесообразно использование мер, предложенных Э. Черных и А. Черных, заключающихся в формировании организациями описи категорий информации, представляющей для них ценность, а также выработке стандартов по распространению этой информации[53].

Меры технического обеспечения.

Данная группа мер включает в себя использование современных программных, программно-аппаратных и аппаратных средств и методов, а также разработку новых эффективных методик предотвращения подготавливаемых преступлений, обнаружения и расследования совершаемой преступной деятельности, а также ликвидации последствий совершенных преступлений. Аппаратные средства включают в себя, в частности, технические устройства для защиты средств компьютерной техники и сетевых средств связи от нежелательных воздействий, для перекрытия нежелательных физических каналов утечки информации, а также устройства для анализа защищенности средств компьютерной техники от внешнего воздействия. Программные средства включают в себя соответствующее программное обеспечение, например, сетевые экраны (брандмауэры) по защите компьютеров и локальных сетей, программы для криптографической защиты и т.д. [54]

---

[52] Аркуша, Л.И. Особенности первоначального этапа расследования компьютерных преступлений / Л.И. Аркуша // Информационные технологии и безопасность: сб. науч. тр. Междунар. конф. – Киев: Национальная академия наук Украины, 2003. – Вып. 3. – С. 3.

[53] Черных, Э. «Компьютерные» хищения: как их предотвратить? / Э. Черных и А. Черных // Советская юстиция. - 1993. - № 3. – С. 21.

[54] Лукацкий, А.В. Обнаружение и предотвращение атак / А.В. Лукацкий // Информационная безопасность. - 2004. -№ 5. - С. 38 – 39.

Меры методического обеспечения.

В качестве методических мер предупреждения компьютерных преступлений выступают, во-первых, создание общей методологии противодействия компьютерной преступности, во-вторых - разработка и апробация конкретных методик предупреждения компьютерных преступлений. Необходимо скорейшее создание надежных и эффективных методик расследования наиболее значимых компьютерных преступлений, например, таких как высокотехнологичные преступления. В силу высокой динамики компьютерной преступности необходимо развитие методов криминалистического прогнозирования[55].

Важной методической мерой является также создание современной учебно-методической базы для подготовки, переподготовки и повышения квалификации сотрудников правоохранительных органов, специализирующихся в области расследования компьютерных преступлений.

Как уже отмечалось выше, отдельные группы мер криминалистического предупреждения тесно связаны друг с другом и предполагают их одновременное применение. Примером является организационно-методическая задача по обеспечению подготовки квалифицированных кадров для правоохранительных органов. Организационная составляющая этой задачи включает объединение усилий специалистов существенно разных профилей (в сфере информационных технологий и в области криминалистики), методическая заключается в разработке новой учебно-методической базы образовательного процесса.

Далее приводимые учебно-методические материалы содержат указания, рекомендации и иную информацию по проведению занятий по учебной дисциплине «Предупреждение компьютерных преступлений», которая

[55] Акиев А.Р. Развитие научных представлений о криминалистическом прогнозировании // Вестник Санкт-Петербургского университета МВД России. - 2023. - № 4 (100). - С. 80-86; Григорьева А.Е. Метод криминалистического прогнозирования в расследовании преступлений // Вестник северо-восточного федерального университета им. М.К. Аммосова. Серия: История. Политология. Право. 2023. - № 4 (32). - С. 12-16.

должна закрывать цикл учебных дисциплин по криминалистическому противодействию компьютерным преступлениям. В материалах содержатся примерные планы семинарских занятий и примерный перечень вопросов для самоконтроля и зачета, представлены темы для подготовки учащимися рефератов и научных докладов, по каждой из тем приведена необходимая для подготовки литература.

Учебно-методические материалы рассчитаны в первую очередь на обучающихся, имеющих минимальное юридическое образование, могут быть использованы слушателями курсов повышения квалификации по юридическим направлениям подготовки.

Темы семинарских занятий отражают последовательность изучения курса и позволяют наиболее полно изучить учебный материал. К каждой теме практического занятия приводятся контрольные вопросы и подробный список дополнительной литературы, которая рекомендуется для изучения. Выбор литературы к теме семинарского занятия определяется необходимостью более глубокого изучения отдельных вопросов темы, обращения к различным научным взглядам.

При подготовке к семинарскому занятию следует изучить Уголовно-процессуальный кодекс РФ, специальные законы, которые регулируют отдельные вопросы уголовно-процессуальной деятельности. В некоторых темах курса следует изучить материалы судебно-следственной практики. Целесообразно изучение экспертных мнений и научно-практических достижений науки криминологии. Эти материалы необходимы для анализа правоприменительной практики, выявления конкретных мер криминалистического предупреждения компьютерных преступлений, их обобщения, классифицирования, анализа.

При изучении курса «Предупреждение компьютерных преступлений» предполагается зачет как форма итогового контроля. В качестве промежуточного контроля предусмотрено выполнение индивидуальных научно-практических заданий и тестирование по отдельным темам.

3.2. ТЕМА 1. ОСНОВЫ КРИМИНАЛИСТИЧЕСКОГО ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ. СУБЪЕКТЫ ПРЕДУПРЕЖДЕНИЯ.

Контрольные вопросы к занятию:

1. Техническая специфика понятийного аппарата криминалистики, необходимая для расследования и предупреждения компьютерных преступлений.
2. Понятие, соотношение и виды предупреждения и профилактики компьютерных преступлений.
3. Понятие и содержание предупреждения компьютерных преступлений.
4. Виды предупреждения и профилактики компьютерных преступлений.
5. Права и обязанности основных субъектов криминалистического предупреждения компьютерных преступлений.

На проведение занятия отводится 4 часа.

Рекомендуемая литература

1. Вехов, В.Б. Возможности правоохранительных органов по противодействию ddos-атакам. Защита информации. Инсайд. - 2008. - № 3. - С. 77-82.
2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО «Издательство «Юрлитинформ», 2001. – 496 с.
3. Воронин, Ю.А. Теоретические основы формирования системы противодействия преступности в России // Криминологический журнал Байкальского государственного университета экономики и права. - 2013. - № 1.

4. Гулян А.Р. Основные направления противодействия компьютерной преступности в Российской Федерации // Российский следователь. – 2009. - № 5. - С. 27-28.

5. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. - 2015. - № 1 (59). –С. 21-41.

6. Золотова Е.В. О международном сотрудничестве в борьбе с преступлениями в сфере компьютерной информации // Успехи в химии и химической технологии». -2007. -№10.

7. Зудин В.Ф. Социальная профилактика преступлений: Криминологические и криминалистические проблемы; под ред. В.И. Федулова. - Аратов: Изд-во Саратовского ун-та, 1983. - 188 с.

8. Иванов И.И. Криминалистическая превенция (генезис, теоретические и методологические основы, перспективы развития в сфере нового уголовно-процессуального законодательства). - СПб.: Изд-во Санкт-Петербургского ун-та МВД России, 2003. - 138 с.

9. Иванов, И. И. Криминалистическая превенция (комплексное исследование генезиса, состояния, перспектив): автореф. дис. … докт. юрид. Наук: 12.00.09. - СПб., 2004. - 36 с.

10. Мазуров, В.А. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий / В.А. Мазуров, В.В. Поляков // Известия Алтайского государственного университета. – 2009. – № 2. – С. 95 - 98.

11. Махтаев, М.Ш. Основы теории криминалистического предупреждения преступлений / М.Ш. Махтаев. - М.: Изд-во «Раритет», 2001. - 272 с.

12. Пархоменко, С.В. Предупреждение компьютерной преступности в российской федерации: интегративный и комплексный подходы / С.В. Пархоменко, К.Н. Евдокимов // Криминологический журнал Байкальского

государственного университета экономики и права. - 2015. - № 2. – С. 265-276.

13. Поляков, В.В. Криминалистическая структура мер предупреждения компьютерных преступлений / В.В. Поляков // Библиотека криминалиста : научный журнал. – 2013. – №5 (10). – С. 287 - 291.

14. Поляков, В.В. Особенности профилактики преступлений в сфере неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации: сб. науч. статей. – Барнаул: Изд-во Алт. ун-та, 2008. – С. 11-16.

15. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : дис. ... канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 247 с.

16. Поляков, В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет / В.В. Поляков // Известия Алтайского государственного университета. – 2016. – № 3 (91). – С. 142-144. ISSN 1561-9443

17. Поляков, В.В. Роль субъектов криминалистического предупреждения преступлений в сфере компьютерной информации / В.В. Поляков, Н.В. Людкова // Уголовно-процессуальные и криминалистические чтения на Алтае. – Барнаул : Барнаульский юридический институт МВД России, 2016. - С. 90-93.

18. Саломатина, Е.С. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности / Е.С. Саломатина // Вестник Владимирского юридического института. – 2011. – №4. – С. 137-141.

19. Стратегия развития информационного общества в Российской Федерации. Утверждена Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 // Российская газета. – 16.02.2008.

20. Чекунов И.Г. Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений // Российский следователь. – 2013. - № 3

21. Эмиров М.Б., Саидов А.Д., Рахимханова Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник ДГУ. – 2011. - №2. С. 63-66.

3.3. ТЕМА 2. ПРИЧИНЫ И УСЛОВИЯ, СПОСОБСТВУЮЩИЕ СОВЕРШЕНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Технические причины и условия, способствующие совершению компьютерных преступлений.
2. Социальные причины и условия, способствующие совершению компьютерных преступлений.
3. Экономические причины и условия, способствующие совершению компьютерных преступлений.
4. Политические причины и условия, способствующие совершению компьютерных преступлений.
5. Психологические причины и условия, способствующие совершению компьютерных преступлений.

На проведение занятия отводится 4 часа.

Рекомендуемая литература

1. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества – М.: Юрлитинформ, 2002. – 496 с.
2. Григорян В.А. Система мер предупреждения преступности. Деятельность государственных органов и общественных организаций по профилактике тунеядства, пьянства, наркомании, рецидивной преступности. Методическое пособие / В.А. Григорян, Н.П. Косоплечев, И.В. Федулов. - М.: ВНИИ укрепления законности и правопорядка,1988. - 128 с.
3. Гулян А.Р. Основные направления противодействия компьютерной преступности в Российской Федерации // Российский Следователь. - 2009. - № 5. – С. 27-28.

4. Доктрина информационной безопасности РФ // Российская газета: сайт. URL: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

5. Мадоян В.В. Виды компьютерной преступности и меры по их противодействию в России // Новый университет. - 2012. - № 2(12).

6. Мазуров, В.А. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий / В.А. Мазуров, В.В. Поляков // Известия Алтайского государственного университета. – 2009. – № 2. – С. 95 - 98.

7. Мазуров, И.Е. Предупреждение хищений, совершенных с использованием интернет-технологий // Актуальные проблемы гуманитарных и естественных наук. - № 11-1. – 2014.

8. Поляков, В.В. Криминалистическая структура мер предупреждения компьютерных преступлений / В.В. Поляков // Библиотека криминалиста : научный журнал. – 2013. – №5 (10). – С. 287 - 291.

9. Поляков, В.В. Особенности профилактики преступлений в сфере неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации: сб. науч. статей. – Барнаул: Изд-во Алт. ун-та, 2008. – С. 11-16.

10. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : автореф. дис. … канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 28 с.

11. Поляков, В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет / В.В. Поляков // Известия Алтайского государственного университета. – 2016. – № 3 (91). – С. 142-144.

12. Поляков, В.В. Результаты анкетирования по делам о неправомерном удаленном доступе к компьютерной информации / В.В. Поляков // Уголовно-процессуальные и криминалистические чтения на Алтае : матер. межрегион. науч.-практ. конф. / под ред. В. К. Гавло. – Барнаул : Изд-во Алт. ун-та, 2008. – Вып. 7. – С. 245 - 249.

13. Поляков, В.В. Роль субъектов криминалистического предупреждения преступлений в сфере компьютерной информации / В.В. Поляков, Н.В. Людкова // Уголовно-процессуальные и криминалистические чтения на Алтае. – Барнаул : Барнаульский юридический институт МВД России, 2016. - С. 90-93.

14. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. - № 24. - С. 43-46.

3.4. ТЕМА 3. ОБСТОЯТЕЛЬСТВА, ПРЕПЯТСТВУЮЩИЕ РАССЛЕДОВАНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Правовые обстоятельства, препятствующие расследованию компьютерных преступлений.
2. Обстоятельства, препятствующие расследованию компьютерных преступлений.
3. Методические обстоятельства, препятствующие расследованию компьютерных преступлений.
4. Технические обстоятельства, препятствующие расследованию компьютерных преступлений.
5. Криминальные обстоятельства, препятствующие расследованию компьютерных преступлений.

На проведение занятия отводится 6 часов.

Рекомендуемая литература

1. Косынкин А.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.09 / А.А. Косынкин. – Саратов, 2012. – 25 с.
2. Мазуров, В.А. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий / В.А. Мазуров, В.В. Поляков // Известия Алтайского государственного университета. – 2009. – № 2. – С. 95 - 98.
3. Поляков, В.В. Анализ обстоятельств, затрудняющих расследование и доказывание преступлений в сфере компьютерной информации / В.В. Поляков // Уголовно-процессуальные и криминалистические чтения на Алтае : матер. Региональной науч.-практ.

конф. / под ред. В.К. Гавло. – Барнаул : Изд-во Алт. ун-та, 2006. – Вып. 6. – С. 111-117.

4. Поляков, В.В. Анализ факторов, затрудняющих расследование неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации : сб. науч. статей. – Барнаул : Изд-во Алт. ун-та, 2008. – С. 17 - 24.

5. Поляков, В.В. Криминалистическая структура мер предупреждения компьютерных преступлений / В.В. Поляков // Библиотека криминалиста : научный журнал. – 2013. – №5 (10). – С. 287 - 291.

6. Поляков, В.В. Некоторые сложности расследования компьютерных преступлений / В.В. Поляков, С.А. Лапин // Совершенствование деятельности правоохранительных органов по борьбе с преступностью в современных условиях : матер. Междунар. научн.-практ. конф. (Тюмень, 1-2 ноября 2013 г.). – Тюмень, 2013. – Вып. 10, Ч. 2. – С. 208-211.

7. Поляков, В.В. Особенности профилактики преступлений в сфере неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации: сб. науч. статей. – Барнаул: Изд-во Алт. ун-та, 2008. – С. 11-16.

8. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации : автореф. дис. … канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 28 с.

9. Поляков, В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет / В.В. Поляков // Известия Алтайского государственного университета. – 2016. – № 3 (91). – С. 142-144.

3.5. ТЕМА 4. МЕРЫ КРИМИНАЛИСТИЧЕСКОГО ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Контрольные вопросы к занятию:

1. Технические меры криминалистического предупреждения компьютерных преступлений.
2. Методические меры криминалистического предупреждения компьютерных преступлений.
3. Организационные меры криминалистического предупреждения компьютерных преступлений.
4. Правовые меры криминалистического предупреждения компьютерных преступлений.

На проведение занятия отводится 10 часов.

Рекомендуемая литература

1. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества – М.: Юрлитинформ, 2002. – 496 с.

6. Гавло, В.К. Криминалистическая деятельность как фактор снижения рисков, связанных с совершением компьютерных преступлений / В.К. Гавло, В.В. Поляков // Социальная безопасность населения юга Западной Сибири – региональные риски и пути повышения эффективности защиты населения региона от природных, техногенных и гуманитарных угроз : матер. Междунар. науч.-практ. конф. / под ред. В.Н. Белоусова. – Барнаул : АзБука, 2005. – Вып. 6. – С. 84-85.

7. Гавло, В.К. Особенности применения информационных технологий при подготовке курсов по расследованию преступлений в сфере компьютерной информации / В.К. Гавло, В.В. Поляков // Единая

образовательная информационная среда: проблемы и пути развития : матер. IV Всерос. науч.-практ. конф. – Томск : Изд-во ТПУ, 2005. – С. 42-43.

2. Гавло, В.К. Специфика обучения кадров органов внутренних дел, расследующих компьютерные преступления / В.К. Гавло, В.В. Поляков // Уголовно-процессуальные и криминалистические чтения на Алтае : матер. Региональной науч.-практ. конф. / под ред. В.К. Гавло. – Барнаул : Изд-во Алт. ун-та, 2006. – Вып. 6 – С. 23-26.

3. Григорян В.А. Система мер предупреждения преступности. Деятельность государственных органов и общественных организаций по профилактике тунеядства, пьянства, наркомании, рецидивной преступности. Методическое пособие / В.А. Григорян, Н.П. Косоплечев, И.В. Федулов. - М.: ВНИИ укрепления законности и правопорядка,1988. - 128 с.

4. Гулян А.Р. Основные направления противодействия компьютерной преступности в Российской Федерации // Российский Следователь. - 2009. - № 5. – С. 27-28.

5. Мазуров, В.А. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий / В.А. Мазуров, В.В. Поляков // Известия Алтайского государственного университета. – 2009. – № 2. – С. 95 - 98.

6. Пак П.Н. Некоторые аспекты прокурорского надзора за расследованием преступлений в сфере компьютерной информации. http://pravgos.narod.ru/html/library/yang_sience/ys_lib_pak_001.htm.

7. Погодин С.Б. Особенности расследования преступлений в сфере компьютерной информации // Российский следователь, 2004. – № 7. – С. 6 – 9.

8. Поляков, В.В. Анализ новых положений уголовного законодательства Российской Федерации в сфере компьютерной информации / В.В. Поляков, А.С. Мананников, Т.В. Лысенко // Гуманитарные науки и образование в Сибири. – 2013. – №2(12). – С. 241-244.

9. Поляков, В.В. К вопросу о повышении эффективности расследования преступлений в сфере компьютерной информации / В.В.

Поляков // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : матер. Четвертой Междунар. науч.-практ. конф. – Барнаул : Изд-во БЮИ МВД России, 2006. – С. 93-94.

10. Поляков, В.В. Криминалистическая структура мер предупреждения компьютерных преступлений / В.В. Поляков // Библиотека криминалиста : научный журнал. – 2013. – №5 (10). – С. 287 - 291.

11. Поляков, В.В. Особенности подготовки кадров, специализирующихся в расследовании компьютерных преступлений / В.В. Поляков // Матер. Второго Пленума СибРОУМО вузов РФ в области информационной безопасности : сб. статей. – Томск : Изд-во «В-Спектр», 2006. – С. 119.

12. Поляков, В.В. Особенности подготовки специалистов для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации / В.В. Поляков // Известия Алтайского государственного университета.– 2010. – N 2/1. – С. 96 - 97.

13. Поляков, В.В. Особенности противодействия кибертерроризму / В.В. Поляков, А.С. Мананников // Информационное противодействие экстремизму и терроризму : Сборник трудов II всероссийской научно-практической конференции (Краснодар, 21 мая 2015 г.) - Краснодар: Краснодарский университет МВД России, 2015. – С. 99-105.

14. Поляков, В.В. Особенности профилактики преступлений в сфере неправомерного удаленного доступа к компьютерной информации / В.В. Поляков // Проблемы правовой и технической защиты информации: сб. науч. статей. – Барнаул: Изд-во Алт. ун-та, 2008. – С. 11-16.

15. Поляков, В.В. Перспективы переподготовки и повышения квалификации сотрудников правоохранительных органов / В.В. Поляков, В.А. Мазуров, А.А. Исаев, Т.В. Сидоренко // Алтай-Азия 2014: Евразийское образовательное пространство - новые вызовы и лучшие практики: матер II Международного образовательного форума (Барнаул, 25–26 сентября 2014 г.). – Барнаул: Изд-во Алт. ун-та, 2014. – С. 82-85.

16. Поляков, В.В. Применение информационных технологий в переподготовке и повышении квалификации сотрудников правоохранительных органов / В.В. Поляков, В.А. Мазуров, А.А. Исаев, Т.В. Сидоренко // Использование цифровых средств обучения и робототехники в общем и профессиональном образовании: опыт, проблемы, перспективы : сб. науч. статей I Всероссийской науч.-практ. конф. с международным участием, Барнаул, 5-6 ноября 2013 г.. – Барнаул : Изд-во Алт. ун-та, 2013. – С. 111-112.

17. Поляков, В.В. Противодействие распространению наркотических средств в интернет-пространстве / В.В. Поляков // Антинаркотическая безопасность. – 2015. – № 1 (4) - С. 68-70.

18. Поляков, В.В. Профилактика экстремизма и терроризма, осуществляемого с помощью сети Интернет / В.В. Поляков // Известия

19. Поляков, В.В. Роль субъектов криминалистического предупреждения преступлений в сфере компьютерной информации / В.В. Поляков, Н.В. Людкова // Уголовно-процессуальные и криминалистические чтения на Алтае. – Барнаул : Барнаульский юридический институт МВД России, 2016. - С. 90-93.

20. Поляков, Вит.В. Использование цифровых средств обучения при подготовке специалистов для правоохранительных органов / Вит.В. Поляков, В.А. Мазуров, В.В. Поляков // Использование цифровых средств обучения и робототехники в общем и профессиональном образовании: опыт, проблемы, перспективы : сб. науч. статей I Всероссийской науч.-практ. конф. с международным участием, Барнаул, 5-6 ноября 2013 г.. – Барнаул : Изд-во Алт. ун-та, 2013. – С. 109-111.

21. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. - № 24. - С. 43-46.

22. Сударева Л.А. Правовое и информационное обеспечение деятельности органов внутренних дел по предупреждению компьютерных

преступлений: автореф. дис. … канд. юрид. наук: 12.00.08 / Л.А. Судерева. – Москва, 2008. – 24 с.

3.6. ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Понятие, соотношение и виды предупреждения и профилактики компьютерных преступлений.
2. Права и обязанности основных субъектов криминалистического предупреждения компьютерных преступлений.
3. Причины и условия, способствующие совершению компьютерных преступлений
4. Обстоятельства, затрудняющие расследование компьютерных преступлений
5. Правовые меры предупреждения компьютерных преступлений
6. Методические меры предупреждения компьютерных преступлений
7. Организационные меры предупреждения компьютерных преступлений
8. Технические меры предупреждения компьютерных преступлений.

3.7. ТЕМЫ РЕФЕРАТОВ И НАУЧНЫХ ДОКЛАДОВ

1. Права и обязанности основных субъектов криминалистического предупреждения компьютерных преступлений.
2. Причины и условия, способствующие совершению компьютерных преступлений
3. Обстоятельства затрудняющие расследование компьютерных преступлений
4. Правовые меры предупреждения компьютерных преступлений
5. Методические меры предупреждения компьютерных преступлений
6. Организационные меры предупреждения компьютерных преступлений
7. Технические меры предупреждения компьютерных преступлений

ЗАКЛЮЧЕНИЕ

Содержащиеся в пособии учебные материалы формируют у обучающихся необходимые знания основ криминалистической методики расследования компьютерных преступлений, понимании общего и особенного в криминалистической характеристике данных преступлений, дают представление о специфике доказательств и доказывания совершения таких преступлений. Эти материалы полезны для изучения криминалистических основ методики расследования, а также для понимания содержания криминалистического предупреждения компьютерных преступлений.

Представленные в учебном пособии материалы, предназначенные для проведения семинарских занятий по дисциплинам цикла криминалистического противодействия компьютерным преступлениям обеспечивает необходимую последовательность в изучении знаний, представленных в виде определенной системы. Такая система в значительной степени повышает качество усвоения материала и возможности его применения на практике. Основным результатом обучения является повышение профессионального уровня будущих сотрудников правоохранительных органов, организаций и учреждений, работа которых будет связана с противодействием компьютерным преступлениям. Конкретными результатами использования комплексного подхода, заложенного в пособии, должны стать знания, умения и навыки, обеспечивающие правильные решения и действия по быстрому и полному установлению обстоятельств компьютерных преступлений, качественный сбор доказательств, эффективное доказывание совершения преступлений в различных криминалистических ситуациях и применение мер предупреждения киберпреступлений.

Использование предложенных учебно-методических материалов по дисциплинам цикла криминалистического противодействия компьютерным

преступлениям способствует улучшению образовательного процесса, содействует его более рациональной организации. Приведенные в учебном пособии сведения могут также оказать помощь в осуществлении контроля знаний учащихся. Объединение теоретических положений с практическими рекомендациями дает положительный эффект в получении устойчивых знаний, умений и навыков, направленных на расследование компьютерных преступлений.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Аносов А.В., Кашапова Е.С. Понятие преступлений в сфере высоких технологий // Академическая мысль (сетевое издание) : интернет-издание. 2018. № 4 (5). С. 15–19. URL: https://mvd.ru/upload/site120/folder_page/010/368/829/AM_4_5_2018.pdf (дата обращения: 15.10.2023). Режим доступа: свободный.

2. Бахтеев Д.В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Российское право: образование, практика, наука : науч. журн. Екатеринбург: Уральский государственный юридический университет им. В.Ф. Яковлева. 2016. № 3 (93). С. 24–26.

3. Бертовский Л.В., Сембекова Б.Р. Высокотехнологичные преступления как угроза национальной безопасности // Новеллы материального и процессуального права: материалы Всерос. (нац.) науч.-практ. конф., Красноярск, 1 мая–1 октября 2020 г. / ред. кол.: Е.А. Ерахтина, С.М. Курбатова, А. Г. Русаков. Красноярск: Краснояр. гос. аграр. ун-т, 2020. С. 127–130.

4. Бессонов А.А. Объект (предмет) преступного посягательства как элемент криминалистической характеристики преступлений / А. А. Бессонов // Вестник Калмыцкого института гуманитарных исследований РАН. – 2014. - № 4. - С. 231.

5. Воронин Ю.А., Беляева И.М., Кухтина Т.В. Современные тенденции преступности в цифровой среде // Вестник Южно-Уральского государственного университета. Серия «Право» : науч. журн. 2021. Т. 21, № 1. С. 7–12.

6. Гавло В.К., Поляков В.В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. – 2006. – №2. – С. 44-48.

7. Гавло В.К., Поляков В.В. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. – 2007. – №5 (57). – С. 146-152.

8. Гребеньков А.А. Преступность в сфере высоких технологий в России: приоритеты борьбы // Известия Юго-Западного государственного университета. Серия История и право : науч. журн. 2014. № 3. С. 72–77.

9. Давыдов С.И., Кондратьев М.В., Поляков В.В. Противодействие транснациональным организованным группам, использующим информационно-коммуникационные технологии для незаконного сбыта наркотических средств // Правоприменение. – 2024. - № 8 (1). – С. 111-120.

10. Давыдов В.О., Тишутина И.В. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. Иркутск: Восточно-Сибирский институт МВД России. 2020. № 2 (14). С. 81–91.

11. Девдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. - № 1 (59). – 2015.

12. Евдокимов К.Н. Анекселенктотичная технотронная преступность (частная теория) // Российский судья : науч. журн. 2018. № 4. С. 35–39.

13. Ищенко Е.П. Криминалистические аспекты расследования киберпреступлений // Уголовное производство: процессуальная теория и криминалистическая практика : мат-лы V междунар. науч.-практич. конф., 27–29 апреля 2017 г., г. Симферополь – Алушта. Симферополь : ИТ «АРИАЛ», 2017. С. 62–65.

14. Ищенко Е.П., Кручинина Н. В. Высокие технологии и криминальные вызовы // Всероссийский криминологический журнал. 2022. Т. 16, № 2. С. 199–206.

15. Козлов В.Е. Об отдельных аспектах криминалистического и оперативно-технического обеспечения противодействия преступлениям, совершаемым с использованием средств компьютерной техники // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сб. статей XVIII Международ. науч.-практич. конф. «Уголовно-процессуальные и криминалистические чтения на Алтае». Вып. XVI / отв. ред. С. И. Давыдов, В. В. Поляков. Барнаул, 2020. С. 20–26.

16. Комаров И.М. «Современный» язык криминалистики // Высокотехнологичное право: современные вызовы : мат-лы IV Международ. межвуз. науч.-практ. конф. (17–20 февраля 2023 года, Москва – Красноярск) / Национальный исследовательский университет «Московский институт электронной техники»; Красноярский государственный аграрный университет. Часть 1. Красноярск, 2023. С. 156–161.

17. Кушниренко С.П. Методика расследования преступлений в сфере высоких технологий : конспект лекций. СПб, 2007. 64 с.

18. Мазуров В.А., Поляков В.В. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий // Известия Алтайского государственного университета. – 2009. – № 2. – С. 95 - 98.

19. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ : монография. Воронеж : Воронежский госуниверситет, 2001. 176 с.

20. Осипенко А.Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 181–188.

21. Поляков В.В. Структура и содержание способа совершения высокотехнологичных преступлений // Российское право: образование, практика, наука. - 2023. - № 1. - С. 27–39.

22. Поляков В.В. Высокотехнологичные преступления: концептуальные основы криминалистической методики расследования // Вестник Томского государственного университета. - 2024. - № 498. - С. 217-225.

23. Поляков В.В. Групповая форма совершения преступлений как один из признаков высокотехнологичной преступности // Российский юридический журнал. – 2023. - № 1 (148). – С. 117-126.

24. Поляков В.В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений // Lex russica. — 2022. — Т. 75. — № 6. — С. 85–96.

25. Поляков В.В. К проблеме криминалистической сложности расследования высокотехнологичных преступлений // Российский следователь. - 2023. - № 11. - С. 7-10.

26. Поляков В.В. Криминалистическая классификация субъектов противодействия расследованию высокотехнологичных преступлений // Актуальные проблемы российского права. — 2023. — Т. 18. — No 2. — С. 178–192.

27. Поляков В.В. Основы формирования криминалистической методики расследования высокотехнологичных преступлений // Уголовное судопроизводство: правовое, криминалистическое и оперативно-розыскное обеспечение : монография / под ред. С.И. Давыдова – Барнаул : Изд-во Алт. ун-та, 2019. – Гл. 2 п. 2.2. – С. 114-126.

28. Поляков В.В. Особенности производства осмотра по компьютерным преступлениям // Российский следователь. - 2017. - № 21. - С. 14-17.

29. Поляков В.В. Понятие «высокотехнологичные преступления» в криминалистике// Криминалистика: вчера, сегодня, завтра. 2023. – Т. 28. – № 4. – С. 151 - 162.

30. Поляков В.В. Применение технологий социальной инженерии при совершении высокотехнологичных преступлений // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. 2023. – Т. 27. – № 3. – С. 175- 188.

31. Поляков В.В. Тенденции развития цифровых средств совершения высокотехнологичных преступлений // Информационное право. – 2023. - №4 (78). – С. 26-28.

32. Поляков В.В., Попов Л.А. Особенности личности компьютерных преступников // Известия Алтайского государственного университета. – 2018. –№ 6 (104). – С. 256-259.

33. Поляков В.В., Маюнов С.И. Проблемы производства судебных компьютерно-технических экспертиз // Евразийский юридический журнал. - 2016. - № 10 (101). – С. 233-235.

34. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2014. - № 2 (32). - С. 162-166.

35. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3. С. 87-99.

36. Россинская Е. Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестник Восточно-Сибирского института МВД России. 2021. № 2 (97). С. 190–200.

37. Семикаленова А.И. Цифровые следы: назначение и производство экспертиз // Вестник университета им. О.Е. Кутафина. 2019. № 5. С. 115-120.

38. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. 2017. № 1 (73). С. 137-140.

39. Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. Т. 17. № 3 (136). С. 102-111.

40. Суходолов А.П., Бычкова А.М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 753–766.

Учебное издание

Поляков Виталий Викторович

ОСНОВЫ МЕТОДИКИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Публикуется в авторской редакции

Оформление обложки *Ю.В. Луценко*

Издательская лицензия ЛР 020261 от 14.01.1997 г.

Подписано в печать 23.08.2024. Дата выхода в свет 28.08.2024.

Формат 60х84 1/16. Бумага офсетная.

Усл.-печ. л. 7,21. Тираж 50. Заказ 434.

Типография Алтайского государственного университета:

656049, Барнаул, ул. Димитрова, 66