АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

· 1973 ·

ЮРИДИЧЕСКИЙ ИНСТИТУТ АГУ

приоритет2030^

лидерами становятся

В.В. Поляков

Методические основы противодействия компьютерным преступлениям

Министерство науки и высшего образования Российской Федерации
Алтайский государственный университет

В.В. Поляков

МЕТОДИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Учебное пособие

Барнаул
Издательство
Алтайского государственного
университета
2024

УДК 343.23:004(075.8)
ББК 67.408.135я73
П 542

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

Поляков, Виталий Викторович.
П 542 **Методические основы противодействия компьютерным преступлениям** : учебное пособие / В.В. Поляков ; Министерство науки и высшего образования РФ, Алтайский государственный университет. — Барнаул : Изд-во Алт. ун-та, 2024. – 83 с.

ISBN 978-5-7904-2862-3.

В пособии приведены теоретические основы противодействия компьютерным преступлениям. Представлены методические рекомендации, материалы и задания для проведения практических занятий по дисциплинам, направленным на обучение противодействию компьютерным преступлениям, а также задания для контроля полученных знаний. Предложена система примерных заданий для изучения научно-практических методов противодействия компьютерной преступности. Эти задания могут быть использованы при прохождения производственной практики учащимися. Представленные методические материалы могут применяться также при повышении квалификации и переподготовке специалистов юридического профиля. Пособие предназначено для преподавателей юридических дисциплин, студентов, обучающимся по юридическим направлениям подготовки ВУЗов, а также специалистов и сотрудников правоохранительных органов, проходящих повышение квалификации.

УДК 343.23:004(075.8)
ББК 67.408.135я73

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

ISBN 978-5-7904-2862-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современное общество столкнулось с проблемой развития и расширяющегося распространения преступлений, совершаемых с использованием информационно-коммуникационных технологий и их низкой раскрываемостью, что ведет к недостаточной обеспеченности защиты граждан от преступных посягательств. По мнению Генерального Прокурора РФ, «правоохранительные органы демонстрируют низкую способность противостоять новому виду преступности»[1]. Во многом это связано с низким профессиональным уровнем должностных лиц правоохранительных органов (следователей, дознавателей, прокуроров, оперативных сотрудников и др.) для эффективного противодействия компьютерным преступлениям. Прежде всего, у сотрудников правоохранительных органов наблюдается недостаток технических знаний в области информационно-коммуникационных технологий. В связи с этим остро требуются современные учебные и научные материалы, раскрывающие закономерности совершения компьютерных преступлений, механизма следообразования электронно-цифровых следов, обстановки преступлений, способов и средств их совершения, знания личностных особенностей преступников и потерпевших, причин и условий, способствующих совершению преступлений и данных в области признаков и особенностей компьютерных преступлений. Существующие криминалистические материалы по противодействию киберпреступности зачастую носят общий характер, оторваны от нужд практики, не адекватны современным способам совершения преступлений.

В условиях цифровизации общества необходимо получение новых и совершенствование имеющихся компетенций, формируемых из знания о современных угрозах со стороны киберпреступности, а также передовых

[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

положений теории и практики расследования и предупреждения таких преступлений. Важным фактором эффективности обучения является практикоориентированный подход, заключающийся в приобретение умений и навыков предупреждения совершения киберпреступлений, а также знания основ расследования киберпреступлений.

Целью учебного пособия являются развитие у обучающихся юридических знаний, умений и навыков по противодействию киберпреступности, а также совершенствование научно-образовательной методов противодействия компьютерным преступлениям с учетом современных научно-педагогических стандартов криминалистической науки, что расширяет педагогические возможности учебного процесса.

Важной составляющей обучения в условиях цифровизации является возможность применения положений настоящего пособия в дистанционных формах обучения.

Учебное пособие содержит теоретические положения, характеризующие особенности рассматриваемой преступной деятельности и основы криминалистического противодействия компьютерным преступлениям. В пособие также включены практические задания для самостоятельной работы по изучению криминалистического противодействия компьютерным преступлениям, задания по производственной практике по основам противодействия компьютерным преступлениям, а также тестовые задания для проведения контроля знаний; библиографического списка; заключения и приложения. Каждый раздел состоит из заданий, отвечающих определенным целям развития соответствующих компетенций у студентов, а также проверке полученных знаний. Так, задания по научно-практическим методам исследования и противодействия компьютерной преступности, призваны помочь в методике сбора, анализа и использования эмпирических и иных данных о компьютерных преступлениях для научно-практического исследования по проблеме противодействия компьютерным преступлениям. Задания для прохождения производственной практики по исследованию

проблем противодействия компьютерным преступлениям позволяют правильно организовать работу по практическому сбору и обобщению судебной практики по компьютерным преступлениям и осуществлению ее криминалистического анализа по эффективной технологии. Тестовые задания позволяют провести контроль знаний студентов по полученным в ходе выполнения предыдущих заданий компетенциям. Таким образом, обучающиеся получают минимальные теоретические знания по проблематике противодействия компьютерным преступлениям, развивают навыки сбора эмпирического материала для исследования (в частности, судебно-следственной практики, анкетного исследования, анализа заключений экспертных мнений), совершенствуют умение проведения научного теоретического, а также практического исследования, а также могут проверить полученные компетенции. В приложениях приводятся примерная анкета для опроса специалистов, участвующих в противодействии компьютерным инцидентам, а также словарь иностранных терминов, применяемых в области информационных технологий.

Глава 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

1.1. ОСНОВНЫЕ ПОЛОЖЕНИЯ МЕТОДИКИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

С конца 90-х годов в России и во всем мире происходит стремительное развитие и распространение информационных технологий. Радикальные изменения в информационных отношениях общества связаны, прежде всего, с применением глобальных компьютерных сетей, в первую очередь, информационной сети Интернет и активной цифровизацией всех сфер человеческой жизни. Особенностью цифровизации и сетевых технологий является то, что они позволяют обеспечить свободный и анонимный доступ к информационным ресурсам одновременно большому числу лиц, находящихся на удалении друг от друга[2]. В силу этого процесс цифровизации общества сопровождается тем, что доступной стала компьютерная техники, которая может быть использована в преступных целях, а также резко увеличилось количество цифровых объектов с недостаточным уровнем защиты. Все эти обстоятельства вызвали резкое обострение криминальной обстановки в информационной сфере общества.

Криминализация информационной сферы нашла свое отражение в появлении высокотехнологичных преступлений, связанных с применением последних достижений науки и техники[3]. Отличительной особенностью данного вида преступности является использование новейших информационных и телекоммуникационных технологий, изобретательное применение новых способов и приемов дистанционно совершаемой

[2] Lederman, E. Law, Information and Information Technology / E. Lederman, R. Shapira. – Nietherland, 2001. – P. 32-76.

[3] Поляков В.В. Понятие «высокотехнологичные преступления» в криминалистике // Криминалистика: вчера, сегодня, завтра: сб. науч. тр. 2023. – Т. 28. – № 4. – С. 151 – 162; Поляков В.В. Тенденции развития цифровых средств совершения высокотехнологичных преступлений / В.В. Поляков // Информационное право. – 2023. - №4 (78). – С. 26-28.

преступной деятельности, рост криминального профессионализма. Эти преступления характеризует исключительно высокий уровень латентности в сочетании с низким уровнем раскрываемости[4]. Важно отметить, что высокотехнологичные преступления быстро развиваются и меняются, что осложняет противодействие им, в том числе со стороны криминалистической науки[5].

Основы криминалистической теории противодействия компьютерным преступлениям были заложены относительно недавно (в конце 90-х – начале 2000-х годов) в работах Ю.М. Батурина, В.Б. Вехова, А.Г. Волеводза, В.В. Голубева, В.Е. Козлова, В.В. Крылова, В.А. Мещерякова, А.Л. Осипенко, Н.Г. Шурухнова и других авторов. Важную роль имели работы Е.Р. Россинской и А.И. Усова.

Законодателем не применяется термин «компьютерные преступления», ставший широко распространенным в современной научной литературе и средствах массовой информации. Данный термин носит доктринальный характер и определяется в криминалистической науке по-разному. Анализ литературы показывает, что содержание этого термина вызывает дискуссии, причем разные авторы вкладывают в него различающийся смысл. Такое положение дел создает несомненные трудности для выработки и применения криминалистических методик и рекомендаций.

Расследование и предупреждение преступлений в сфере компьютерной информации является сложной комплексной проблемой. Для выяснения сути произошедшего преступления и обстоятельств, входящих в предмет установления и доказывания правоохранительным органам требуются специфические знания, находящихся на стыке юриспруденции и компьютерных технологий.

---

[4] Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: ООО Изд-во «Юрлитинформ», 2002. – 496 с.

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

Методики расследования компьютерных преступлений состоит из двух подсистем: криминалистической характеристики преступления и криминалистической характеристики расследования преступления.

Для расследования компьютерных преступлений в связи с их сложностью существенно возрастает роль криминалистической теории, объясняющей различные аспекты преступной деятельности и предлагающей эффективные пути противодействия ей. Одной из базовых криминалистических категорий является криминалистическая характеристика преступлений, которая рассматривается как часть методики расследования преступлений и содержит обобщенные научно обоснованные представления о криминалистически значимых признаках определенных преступлений. В ее рамках происходит поиск и нахождение ответов на вопросы, возникающие в ходе расследования, в частности: что происходит при совершении отдельных видов преступлений; кто и как их совершает; какие и где остаются следы – последствия содеянного; в какой связи они находятся друг с другом; в какой обстановке и в какой криминальной ситуации разворачивалось событие преступления, что способствовало преступной деятельности и т.п. Обобщенная и приведенная в строгую научную систему знаний такая информация составляет суть криминалистической характеристики преступлений.

Однако в криминалистической теории имеются не решенные вопросы и противоречия при определении количества и содержания элементов криминалистической характеристики компьютерных преступлений, прежде всего таких как: личность преступников (особенности группового субъекта) и потерпевших, способах и средствах преступления, специфики следовой картины, причинах и условиях, способствующих совершению преступлений, преступном результате и иных. Во многом это связано с тем, что разные авторы вкладывают отличающийся смысл в понятие компьютерных преступлений, как уже ранее отмечалось. Компьютерные преступления, как явление, слишком широкое и включает в себя большое количество

разновидностей преступлений, имеющих существенные отличия между собой. Отсюда при широком обобщении и абстракции теоретических моделей элементов криминалистической характеристики компьютерных преступлений внутри них возникают закономерные противоречия. Так, например, личностные качества мошенника в сфере компьютерной информации будут существенно отличаться от свойств личности создателя вредоносного программного обеспечения. Более того, внутри одной разновидности преступлений также могут наблюдаться значительные отличия, например, в особенностях личности исполнителя и организатора преступной деятельности.

В настоящее время криминалистическая теория встречается со значительными трудностями в формировании криминалистической характеристики высокотехнологичных преступлений, в сборе и анализе судебной практики по таким делам и относительно малом ее количестве, в сложности понимания механизмов высокотехнологичных преступлений, особенно в части новых средств, используемых при их совершении, в крайне высокой латентности таких преступлений и противодействии расследованию, сложностях сбора цифровых следов преступной деятельности и многих иных обстоятельствах[6].

Знания о типовых моделях элементов криминалистической характеристики преступлений дает возможность выдвигать криминалистические версии об обстоятельствах подлежащих установлению и доказыванию, поскольку все элементы находятся в состоянии зависимости: причинно-следственной (прямой и закономерной) или корреляционной (не прямой, но достаточно вероятной). Так, знание специфики функционирования сложного оригинального программного средства преступления может

[6] Поляков В.В. К проблеме криминалистической сложности расследования высокотехнологичных преступлений / В.В. Поляков // Российский следователь. - 2023. - № 11. - С. 7-10; Поляков В.В. Криминалистическая классификация средств высокотехнологичных преступлений / В.В. Поляков // Вестник Санкт-Петербургского университета. Право. – Т 15. - № 2. - С. 421-439.

позволить сузить круг подозреваемых до тех, кто обладают знаниями и навыками работы с такими средствами.

Аналогично криминалистической характеристике преступлений существует криминалистическая характеристика расследования преступлений, также являющаяся теоретической моделью, но которая 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.

Рассмотренные обстоятельства свидетельствуют об актуальности изучения криминалистических аспектов нового быстро расширяющегося вида преступлений – компьютерных преступлений. Эти аспекты изложены в настоящем учебном пособии.

1.2. ПОНЯТИЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Криминалистическая характеристика преступлений отражает закономерности способов и следообразования преступной деятельности субъекта по приготовлению, совершению и сокрытию преступлений. Формирование теоретических моделей элементов криминалистической характеристики компьютерных преступлений происходит путем обобщения судебно-следственной практики и иных источников информации.

В теории криминалистики нет единого определения криминалистической характеристики преступлений. 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»[7]. По мнению Р. С. Белкина в криминалистическую характеристику преступлений следует включать «характеристику исходной информации, систему данных о способе 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)»[8]. 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[9]. В большинстве

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

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

[9] Бессонов А.А. Частная теория криминалистической характеристики преступлений // автореферат диссертации на соискание ученой степени доктора юридических наук / Акад.

криминалистических исследований последних лет криминалистическая характеристика преступлений справедливо рассматривается как теоретическая модель[10].

Конкретный перечень элементов криминалистической характеристики преступлений в криминалистической науке является дискуссионным. Однако в качестве криминалистически значимой информации может 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 и отношений между субъектами преступления и обстановкой совершения преступления, соучастниками, свидетелями, потерпевшими; наступившими последствиями преступного посягательства; следов-последствий преступлений и других источников информации[11].

Для различных видов преступлений существует свой набор элементов криминалистической характеристики преступлений, который может отличаться не только по их значимости, но и по количеству.

Криминалистические характеристики преступлений могут отличаться в зависимости от критерия классифицирования. Так, в зависимости от уровня обобщения в криминалистике выделяются родовые, групповые, видовые, межвидовые, базовые, усеченные, сквозные и многие иные виды криминалистических характеристик преступлений[12]. При этом, чем уже

упр. МВД РФ. Москва, 2017. С. 11.

[10] 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.

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

[12] 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. –

уровень обобщения преступлений, тем конкретнее по ним данные и выше практикоориентированность такой характеристики в методики его расследования. Выделенные в теоретических целях элементы криминалистической характеристики преступлений находятся в неразрывной связи друг с другом и отсюда имеют причинно-следственные и корреляционные зависимости. 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. С помощью криминалистической характеристики преступлений оказывается непосредственное влияние на построение оптимальной криминалистической методики расследования и 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[13].

М.: Академия управления МВД России, 2022. Ч. 1. С. 54-62.

[13] 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.

1.3. ДОКАЗЫВАНИЕ ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Наименее разработанными и одновременно одними из наиболее сложных являются вопросы доказывания преступлений, совершенных в сфере компьютерной информации, в особенности высокотехнологичных преступлений[14].

Процесс доказывания является основой установления истины по уголовному делу и строится на преимущественном оперировании полученными в ходе следствия доказательствами[15]. Процесс доказывания в случае компьютерных преступлений затрудняется слабой разработанностью вопросов, связанных с применимостью, относимостью и допустимостью используемых электронных доказательств.

В суде подлежат доказыванию следующие обстоятельства: событие преступления; объект; предмет; способ; место, время; размер и вид ущерба; 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, которые могут использоваться в судебном процессе по делам о преступлениях в сфере компьютерной информации. Согласно ст. 74 УПК РФ, к доказательствам отнесены: показания подозреваемого, обвиняемого, показания потерпевшего, свидетеля; заключение и показания эксперта; заключение и показания специалиста; вещественные доказательства;

---

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

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

протоколы следственных и судебных действий; иные документы. 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.

В настоящее время наиболее адекватной развитию криминалистической теории и судебно-следственной практики для характеристики формы электронных доказательств является понятие «электронный документ». Согласно 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»[16].

Понятия «электронный документ» и «электронное доказательство» вызывают 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»[17].

Одной из трудностей, связанных с использованием в качестве доказательств электронных документов, является то обстоятельство, что «при наличии нескольких средств доказывания письменным документам отдается предпочтение, ввиду надежности их исследования и простоты

[16] 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.

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

непосредственного восприятия органами чувств человека»[18]. С таким положением справедливо не соглашается Р.Г-В. Локк, указывая, что «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»[19].

Электронный документ, содержащий компьютерную информацию, может быть использован в качестве электронного доказательства лишь при точном указании источников этой информации. В качестве источников могут выступать различные носители информации.

Отдельного рассмотрения заслуживает вопрос об объектах носителях следов преступлений. По общему криминалистическому правилу, объекты со следами преступления должны изыматься в оригинале и в натуре. Таким образом, когда это возможно, они изымаются в приоритетном порядке по сравнению с их копями, слепками и т.п. Однако носители компьютерной информации обладают спецификой и изъять информацию вместе с носителем не всегда представляется возможным. Осложняет работу с электронным документом, выступающим в качестве доказательства, отсутствие его однозначной привязки к конкретному носителю компьютерной информации[20]. 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. Как считает Р.Н. Мылицин, «не применимо сочетание таких терминов, как оригинал и копия - могут лишь существовать идентичные по своему содержанию копии одного электронного документа на разных носителях,

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

[19] Там же. С. 18.

[20] 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.

отличающиеся между собой разве что датой создания»[21]. Электронные документы физическими характеристиками практически не обладают и могут быть совершенно 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. Очевидно, что указанную особенность электронных документов необходимо специально учитывать при доказывании по делам о преступлениях в сфере компьютерной информации.

Нужно признать, что полноценное использование электронных доказательств в суде затруднено из-за неразработанности нормативной базы, не успевающей за изменениями компьютерных преступлений и способов их совершения в частности. Сложившиеся противоречия и неопределенности, отсутствие единого понимания ключевых понятий и терминов затрудняют процесс доказывания и требуют скорейшего разрешения.

Криминалистические исследования противодействия компьютерной преступности подвержены достаточно быстрому устареванию. Например, бурное развитие сетевых технологий привело к повсеместному применению беспроводных технологий передачи компьютерной информации, активно развиваются технологии машинного обучения, ведущие к появлению «усиленного» искусственного интеллекта, также стремительно развиваются

[21] Там же.

квантовые технологии и робототехника[22]. Следовательно, от современной криминалистики с одной стороны требуется изучение подобных объектов, а с другой – перечисленные технологии необходимо использовать в криминалистической деятельности[23].

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

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

ГЛАВА 2. ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ИЗУЧЕНИЮ КРИМИНАЛИСТИЧЕСКОГО ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

2.1. ВВЕДЕНИЕ

Задания содержат методические материалы, рекомендации и иную учебную информацию, позволяющую обучающимся повысить эффективность самостоятельной работы по изучению возможностей криминалистического противодействия компьютерной преступности. Предлагаются актуальные темы учебно-исследовательских работ, даются общие методические рекомендации по проведению такой работы и изучению в ходе нее судебно-следственной практики, также предлагаются рекомендации по форме подготовки проекта научно-исследовательской работы.

Задания можно использовать при организации учебно-исследовательской работы учащихся. Эти задания могут также применяться для повышения эффективности контроля знаний преподавателем, в том числе при занятиях, осуществляемых в дистанционной форме.

2.2. ПОДГОТОВКА УЧЕБНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Задание заключается в подготовке проекта научной статьи по предложенному списку тем.

ПРИМЕРНЫЕ ТЕМЫ УЧЕБНО-ИССЛЕДОВАТЕЛЬСКИХ РАБОТ

1. О соотношении "расследования преступлений" и "раскрытия преступлений" на примере компьютерных преступлений
2. Криминалистические особенности новых способов преступлений, совершаемых с использованием информационных технологий
3. Использование машинного обучения (искусственного интеллекта) в качестве средства совершения преступлений
4. Особенности группового совершения компьютерных преступлений
5. Преступный результат как элемент криминалистической характеристики компьютерных преступлений.
6. Особенности противодействия расследованию компьютерных преступлений
7. Обстоятельства, подлежащие установлению и доказыванию по делам о преступлениях в сфере компьютерной информации: теоретические и практические проблемы
8. Следственные версии и планирование расследования по делам о преступлениях в сфере компьютерной информации.
9. Поводы, основания и особенности возбуждения уголовных дел по компьютерным преступлениям.
10. Особенности проведения отдельных ОРМ по компьютерным преступлениям
11. Следственные ситуации и их разрешение в ходе предварительного расследования компьютерных преступлений
12. Негативные обстоятельства по компьютерным преступлениям

13. Криминалистическая техника, используемая в ходе следственных действий по компьютерным преступлениям.

14. Особенности организации расследования компьютерных преступлений

15. Особенности и проблемы тактики производства менее распространенных следственных действий по компьютерным преступлениям (очной ставки, следственного эксперимента, контроля и записи переговоров, получения информации о соединениях между абонентами и (или) абонентскими устройствами)

16. Проблемы расследования компьютерных преступлений на различных этапах криминалистической деятельности

17. Особенности первоначального этапа расследования компьютерных преступлений

18. Особенности начального этапа расследования компьютерных преступлений

19. Особенности последующего этапа расследования компьютерных преступлений

20. Особенности заключительного этапа расследования компьютерных преступлений

21. Анализ практики правоприменения в области расследования компьютерных преступлений

22. Особенности тактических комбинаций и операций по компьютерным преступлениям

23. Анализ нераскрытых компьютерных преступлений и ошибок в их расследовании

24. Особенности судебных ситуаций и их разрешения по делам о компьютерных преступлениях

25. Криминалистическое исследование машинного обучения (искусственного интеллекта) в преступной деятельности и в деятельности по расследованию преступлений

26. Особенности сокрытия компьютерных преступлений и противодействия расследованию

27. Организация и особенности проведения предварительной проверки заявлений и сообщений о преступлениях в сфере компьютерной информации.

28. Региональные особенности компьютерной преступности

29. Особенности транснациональной компьютерной преступности

30. Криминальные ситуации совершения компьютерных преступлений

31. К вопросу о понятии «компьютерная криминалистика»

32. Понятие и особенности высокотехнологичных преступлений

33. Особенности криминалистической латентности компьютерных преступлений

34. Содержание и структура криминалистического предупреждения компьютерных преступлений

35. Криминалистическая характеристика компьютерных преступлений

36. Криминалистическая характеристика расследования компьютерных преступлений

37. Способы совершения компьютерных преступлений

38. Обстановка совершения компьютерных преступлений

39. Особенности личности преступников и потерпевших по делам о компьютерных преступлениях

40. Средства совершения компьютерных преступлений

41. Специфика следовой картины по преступлениям, предусмотренным статьями: 159.6/ 272/ 273/ 274/ 274.1/ 274.2 УК РФ

42. Особенности подготовки компьютерных преступлений

43. Особенности оперативно-розыскной деятельности по компьютерным преступлениям

44. Использование специальных познаний при расследовании компьютерных преступлений

45. Особенности тактики проведения следственных действий по компьютерным преступлениям

46. Организация и проведение осмотра по компьютерным преступлениям, отграничение от иных следственных действий

47. Проблемы производства обыска и выемки компьютерной информации

48. Тактика допроса подозреваемого (обвиняемого) в компьютерном преступлении

49. Проблемы тактики допроса потерпевших и свидетелей по делам о компьютерных преступлениях

50. Особенности доказывания и доказательств по компьютерным преступлениям

ОБЩИЕ МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ ТЕКСТА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Предлагается для ознакомления не плохой практикоориентированный курс: https://intuit.ru/studies/courses/11980/1160/info. В нем последовательно раскрывается процесс подготовки различных видов исследовательских работ, выполняемых в процессе обучения по направлению "Бизнес-информатика", что накладывает свою специфику, но она не критична. Изложены общие теоретические основы, примеры, разбор типичных ошибок. Представлены таблицы, рисунки, схемы, обеспечивающие наглядное восприятие материала. Подробнее можно ознакомиться, в частности, в следующих материалах:

- методологический аппарат научного исследования https://intuit.ru/studies/courses/11980/1160/lecture/18284;
- выбор темы и планирование исследовательской работы https://intuit.ru/studies/courses/11980/1160/lecture/18286;
- методические рекомендации по написанию исследовательских работ https://intuit.ru/studies/courses/11980/1160/lecture/18288.

Полезные **Интернет-сайты** для всех юристов: судебные решения, акты госорганов, правовые базы, информационные ресурсы.

- http://ksrf.ru/ - официальный сайт Конституционного Суда РФ
- http://supcourt.ru/ - официальный сайт Верховного Суда РФ
- http://www.gcourts.ru/ - поиск решений судов общей юрисдикции
- http://rospravosudie.com/ - картотека юристов, адвокатов, судей и судебных решений
- http://sudact.ru/ - судебные и нормативные акты РФ, поиск судебных решений
- http://судебныерешения.рф - поиск решений судов общей юрисдикции
- http://media-pravo.info/ - база данных российской судебной практики по информационному праву
- Юридические социальные сети:
- http://zakon.ru/ - первая социальная сеть для юристов
- http://pravo.ru/ - юридический портал

РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ СУДЕБНО-СЛЕДСТВЕННОЙ ПРАКТИКИ

Судебную практику можно изучить на следующих сайтах:

- https://sudact.ru
- https://sudrf.ru/
- https://actofact.ru/
- https://судебныерешения.рф

и других.

Образец оформления сноски на судебную практику:

Уголовное дело 1-329/2013 // Архив Центрального районного суда г. Барнаула. // https://... (дата обращения: …)

Приговор Якутского городского суда Республики Саха (Якутия) от 26.08.2019 № 1-681/2019 по делу № 1-1462/2018 // https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения:…)

Обязательно необходимо добавить ссылку на страницу сайта, откуда были взяты процессуальные акты.

ФОРМА ПОДГОТОВКИ ПРОЕКТА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Обязательно следует **согласовать** планируемую тему, чтобы не было повторов с другими студентами.

Требование – **оригинальность** (не менее 75%) по системе «Антиплагиат». Плагиата не должно быть ни 1%, то есть нужны:

- кавычки (при полном цитировании текста и сноска на соответствующую страницу);

- или сноска (при пересказе своими словами чужих мыслей).

Целесообразно периодически проверять работу по системе «АНТИПЛАГИАТ» и конечный вариант следует проверить на полной версии программы.

Общее оформление - как научной статьи, во многом аналогично ВКР (цитирование, сноски, библиографический список). Объем не более 5 страниц.

Оформление. Поля: 15 мм. Отступ – 1, интервал -1. **Структура статьи.** ФИО (полностью). Данные об авторе (место работы, ученая степень, ученое звание, город, страна). Название статьи - шрифт -полужирный, буквы прописные, выравнивание по центру. Аннотация, ключевые слова. **Текст статьи**. Шрифт –Times New Roman, размер шрифта -12, начертание - обычный, выравнивание по ширине. Литература – не менее 10 источников и 5 дел судебной практики.

Использование судебной практики в качестве источника данных является обязательным.

Целесообразно использовать **иллюстративный материал**, например, схемы, диаграммы. Приветствуется подготовка презентации по статье для доклада.

2.3. ПРОВЕДЕНИЕ АНКЕТНОГО ИССЛЕДОВАНИЯ И АНАЛИТИЧЕСКОЕ ОБОБЩЕНИЕ ЭКСПЕРТНЫХ МНЕНИЙ

В рамках данного задания необходимо осуществить сбор эмпирических данных. С этой целью учащимся предоставляется выбор либо самостоятельно провести анкетное исследование специалистов, либо проанализировать и обобщить существующие экспертные мнения на основе опубликованных данных.

ПРОВЕДЕНИЕ АНКЕТНОГО ИССЛЕДОВАНИЯ

Задание заключается в анкетировании сотрудников правоохранительных органов и специалистов, встречающихся с угрозами компьютерных преступлений, и в анализе полученных результатов, а также в представлении выводов в виде таблиц, графиков и т.п. Для этого необходимо разработать и применить анкету с актуальными вопросами, требующими выяснения.

АНАЛИТИЧЕСКОЕ ОБОБЩЕНИЕ ЭКСПЕРТНЫХ МНЕНИЙ

Задание заключается в сборе и анализе эмпирических данных в виде экспертных мнений. На основе изучения эмпирических данных (не научных статей), **аналитических отчетов** организаций, занимающиеся информационной безопасностью (например, https://www.facct.ru/, group-ib pdf, PositiveTechnologies, https://bi.zone/ru/, https://rt-solar.ru/events/blog/, https://innostage-group.ru/press/blog/, https://www.infosec.ru/press-center/media-arhive/ и иных) необходимо выявить проблемы расследования высокотехнологичных компьютерных преступлений (*высокотехнологичные преступления – это преступные деяния, совершаемые высокотехнологичным способом, включающим элементы подготовки, совершения и сокрытия следов преступления и преступников, осуществляемые преступной группой, путем применения специально созданных или модифицированных в преступных целях программных, программно-аппаратных или аппаратных средств, с использованием дистанционного доступа к объекту преступного посягательства, сопровождаемые противодействием расследованию,*

отличающиеся высокой латентностью и криминалистической сложностью расследования). При этом научную литературу использовать НЕЛЬЗЯ, так как выводы должны быть авторскими и основанными исключительно на изучении экспертных мнений. На каждый полученный вывод из **экспертного отчета** следует ссылаться, например:

Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. III квартал 2022 года // Центральный Банк Российской Федерации: офиц. сайт. URL: https://www.cbr.ru/statistics/ib/review_3q_2022/ (дата обращения: 13.06.2023). Режим доступа: свободный.

2.4. АНАЛИЗ СУДЕБНОЙ ПРАКТИКИ

Задание заключается в сборе и анализе судебной практике по высокотехнологичным преступлениям (не простым случаям компьютерных преступлений, например, неправомерной выдаче персональных данных и предметов сотрудниками операторов связи и др. организаций посторонним лицам; «взлому» и установке нелицензионных программ, например, случаях признания судом так называемых “патчей”, “кейгенов” и “активаторов”, используемых для “взлома” лицензионного программного обеспечения, в качестве вредоносных программ, а также иных примитивных дел). Поиск и анализ должен быть в отношении *высокотехнологичных преступлений – то есть преступным деяниям, совершаемым высокотехнологичным способом, включающим элементы подготовки, совершения и сокрытия следов преступления и преступников, осуществляемым преступной группой, путем применения специально созданных или модифицированных в преступных целях программных, программно-аппаратных или аппаратных средств, с использованием дистанционного доступа к объекту преступного посягательства, сопровождаемого противодействием расследованию и отличающимся высокой латентностью и криминалистической сложностью расследования*). На примерах не менее 5-10 конкретных уголовных дел (с обязательными ссылками на них) необходимо осуществить криминалистический анализ, чтобы были получены авторские выводы об особенностях тактики/техники/методики расследования:

1. выявить имеющиеся проблемы и особенности предварительной проверки, предварительного расследования и судебного следствия, криминалистического предупреждения преступлений;
2. какие встречались криминальные, следственные и судебные ситуации;
3. какие имелись проблемы выявления, фиксации, изъятия, хранения, исследования, оценки цифровых следов;

4. как эти источники использовались в доказывании;

5. исследовать тактику производства конкретных следственных действий, особенно, не типичных;

6. какие и как в следственных действиях применялись тактические приемы;

7. выявить используемые тактические комбинации и операции;

8. в каких следственных действиях имелись сложности, были допущены ошибки, упущения, какие из них по уголовным делам более типичны;

9. какие были удачные тактические решения;

10. анализ применения криминалистической тактики судом и гособвинителем;

11. особенности тактики защиты;

12. какие у Вас в связи с проведенным анализом уголовных дел имеются предложения, рекомендации.

ТЕХНОЛОГИЯ АНАЛИЗА СУДЕБНОЙ ПРАКТИКИ

Первоначально необходимо изложить фабулу дела, то есть кратко описать то, в чем заключалось преступление и сделать сноску на источник судебной практики с указанием страницы сайта.

1. БЛОК, КАСАЮЩИЙСЯ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ.

1. особенности личности преступников и потерпевших;

2. количество участников и особенности их ролей в преступной группе;

3. особенности способа совершения преступления;

4. особенности средств совершения преступления;

5. особенности следовой картины;

6. причины и условия, способствовавшие совершению преступления;

7. особенности обстановки преступления (мест где находились преступники и потерпевшие при совершении преступления);

8. в чем проявлялось противодействие расследованию

2. БЛОК, КАСАЮЩИЙСЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ НА ЭТАПАХ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ.

1. какие были поводы и основания для возбуждения уголовного дела;
2. особенности предварительной проверки;
3. какие были результаты ОРД;
4. какие особенности были в следственных действиях;
5. какие производились экспертизы;
6. какие были тактические операции и комбинации;
7. когда подозреваемый/обвиняемый признался.
8. была ли совокупность преступлений и по каким статьям УК РФ.

3. БЛОК, КАСАЮЩИЙСЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ НА ЭТАПАХ СУДЕБНОГО РАССЛЕДОВАНИЯ.

1. было ли соглашение о сотрудничестве, без судебного следствия;
2. какие были судебные ситуации по тактике защиты;
3. какие доказательства были отклонены;
4. какие ходатайства заявлялись;
5. какие новые судебные действия проводились;
6. какие были получены новые доказательства;
7. отказ от обвинения по каким статьям;
8. что не смогло доказать обвинение;
9. когда подсудимый признался;
10. была ли доказана совокупность преступлений и по каким статьям УК РФ;
11. Были приняты меры по криминалистическому предупреждению преступлений

Практику можно изучить, в частности, на следующих **сайтах**:

- https://sudact.ru
- https://actofact.ru
- https://sudrf.ru

- https://судебныерешения.рф

и других.

Обязательно необходимо добавить ссылку на страницу сайта, откуда были взяты процессуальные акты. Исследуемые акты надо добавить в качестве приложения в конце документа. Персональные данные фигурантов уголовных дел необходимо обезличить.

Образец оформления сноски на рассмотренные дела:

Уголовное дело 1-329/2013 // Архив Центрального районного суда г. Барнаула. http://... (дата обращения:…)

Приговор Советского районного суда г. Томска от 09.12.2019 по делу № 1-25/2019 // http://sudact.ru... (дата обращения:…)

ГЛАВА 3. ОРГАНИЗАЦИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ ПО ПРОТИВОДЕЙСТВИЮ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

3.1. ОБЩИЕ РЕКОМЕНДАЦИИ ПО ПРОХОЖДЕНИЮ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Перед прохождением практики необходимо определиться с местом ее прохождения, которым может быть:

1. Организация:

1.1. В которой обучающийся *трудоустроен*, работая по юридической специальности;

1.2. С которой заключен *гражданско-правовой договор по оказанию ей юридических услуг;*

1.3. По индивидуальному договору на прохождение практики.

2. Суд общей юрисдикции.

3. Кафедра вуза.

Следует заполнить и сдать на кафедру **Заявление** с указанием желаемого места прохождения. Проходящие практику по договору с организацией должны обязательно приложить два его оригинала к заявлению. Студенты, которые не сдадут заявление (и договор, когда заключение необходимо) **до 04.05.2024г.**, будут распределены в соответствии с общим порядком. В дальнейшем без изменения Приказа **ректора** поменять место практики будет невозможно. Также нельзя будет при пересдаче зачета пройти практику в каком-либо ином месте, например, на кафедре. Студентам, которым необходимо прохождение практики за пределами **города** (то есть **выездная** практика), необходимо также предоставить **второе** Заявление на прохождение **выездной** практики, заполненное на имя **ректора** (с официальным наименованием организации и указанием места прохождения практики***).***

Проходящие практику по трудоустройству (гражданско-правовому договору) со своей организацией договор на практику не заключают, поэтому от них требуется только заявление (и второе Заявление на прохождение выездной учебной практики, если прохождение не в г. Барнауле) с официальным наименованием организации и указанием места прохождения практики.

При прохождении практики в суде общей юрисдикции по направлению от учебного заведения необходимо указать наименование суда и его местонахождение.

3.2. РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ ОТЧЕТНЫХ ДОКУМЕНТОВ ПО РЕЗУЛЬТАТАМ ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ПРЕДОСТАВЛЯЕМЫХ ПО РЕЗУЛЬТАТАМ ПРОХОЖДЕНИЯ ПРАКТИКИ

1. РАБОТАЮЩИМ ПО ЮРИДИЧЕСКОЙ СПЕЦИАЛЬНОСТИ ИЛИ ПО ГРАЖДАНСКО-ПРАВОМУ ДОГОВОРУ НА ОКАЗАНИЕ ЮРИДИЧЕСКИХ УСЛУГ

Список предоставляемых документов:

1) титульный лист отчета:

- по прохождению практики в организации по месту работы (с подписями и печатью);

2) Копия **трудовой книжки** / трудового договора / служебного контракта / **гражданско-правого договора на оказание юридических услуг** выписки из приказа о назначении общественным помощником в СК или органах прокуратуры.

Копия должна содержать запись о работе *«по настоящее время»,* подпись и печать руководителя, а также быть заверена последним днем практики.

3) Характеристика с места работы с подписью и печатью руководителя. Выдается последним днем практики.

Студенты, трудоустроенные, но не по специальности, должны подтвердить юридическую составляющую своей работы, например, приложив должностную инструкцию, в которой это указано и отмечено.

2. ПРОХОДЯЩИМ ПРАКТИКУ ПО НАПРАВЛЕНИЮ (ИНДИВИДУАЛЬНОМУ ДОГОВОРУ)

Практика может быть реализована путем направления в суд общей юрисдикции.

Список предоставляемых документов:

1) Дневник. В процессе прохождения практики обучающимся необходимо ежедневно вести дневник, в который вносятся записи об ежедневно проделанной работе в строгом соответствии с программой практики и индивидуальным заданием. Раздел «Инструктаж по технике безопасности» удостоверяется **подписью** студента. Раздел «Ежедневные записи студентов по практике» должен содержать запись об ежедневно выполненной работе с подробным ее описанием.

2) Отчет о прохождении практики. Отчет по практике должен отражать проделанную работу в период прохождения практики в соответствии с ее программой и заданием. Во всех фигурирующих в отчете документах **не должно содержаться** сведений, составляющих государственную, служебную, коммерческую, личную тайну (включая персональные данные граждан).

Отчет по практике включает следующие **элементы:**

- титульный лист;
- содержание;
- ведение дневника;
- основная часть в соответствии с программой практики и заданием;
- заключение;
- список использованных источников (процессуальных актов);
- приложение (все исследуемые акты прикладываются в приложение).

Основное **задание** практики заключается в сборе и анализе судебной практики по компьютерным преступлениям. На примерах конкретных уголовных дел (с обязательными ссылками на них) необходимо осуществить их криминалистический анализ, чтобы были получены выводы об особенностях тактики/техники/методики расследования:

1. выявить имеющиеся проблемы и особенности предварительной проверки, предварительного расследования и судебного следствия, криминалистического предупреждения преступлений;

2. какие встречались криминальные, следственные и судебные ситуации;

3. какие имелись проблемы выявления, фиксации, изъятия, хранения, исследования, оценки цифровых следов;

4. как эти источники использовались в доказывании;

5. исследовать тактику производства конкретных следственных действий, особенно, не типичных;

6. какие и как в следственных действиях применялись тактические приемы;

7. выявить тактические комбинации и операции;

8. в каких следственных действиях имелись сложности, были допущены ошибки, упущения, какие из них по уголовным делам более типичны;

9. какие были удачные тактические решения;

10. анализ применения криминалистической тактики судом и гособвинителем;

11. особенности тактики защиты;

12. какие у Вас в связи с проведенным анализом уголовных дел имеются предложения, рекомендации...

Практику можно изучить на сайтах:

https://sud-praktika.ru/precedent/category/299.html

https://sudact.ru

https://sudrf.ru/

и иных.

3) Проекты процессуальных документов (3 шт.). Не должны содержать персональные данные.

3. ПРОХОДЯЩИМ ПРАКТИКУ НА КАФЕДРЕ

Список предоставляемых документов:

1) Дневник. В процессе прохождения практики обучающимся необходимо ежедневно вести дневник, в который вносятся записи об ежедневно проделанной работе в строгом соответствии с программой практики и индивидуальным заданием. Раздел «Инструктаж по технике безопасности» удостоверяется **подписью** студента. Раздел «Ежедневные записи студентов по практике» должен содержать запись об ежедневно выполненной работе с подробным ее описанием.

2) Отчет о прохождении практики. Отчет по практике должен отражать проделанную работу в период прохождения практики в соответствии с ее программой и заданием. Во всех фигурирующих в отчете документах **не должно содержаться** сведений, составляющих государственную, служебную, коммерческую, личную тайну (включая персональные данные граждан).

Отчет по практике включает следующие **элементы**:

- титульный лист;
- содержание;
- ведение дневника;
- основная часть в соответствии с программой практики и заданием;
- заключение;
- список использованных источников (процессуальных актов);
- приложение (все исследуемые акты прикладываются в приложение).

Основное **задание** практики заключается в сборе и анализе судебной практики по компьютерным преступлениям. На примерах конкретных уголовных дел (с обязательными ссылками на них) необходимо осуществить их криминалистический анализ, чтобы были получены выводы об особенностях тактики/техники/методики расследования:

1. выявить имеющиеся проблемы и особенности предварительной проверки, предварительного расследования и судебного следствия, криминалистического предупреждения преступлений;

2. какие встречались криминальные, следственные и судебные ситуации;

3. какие имелись проблемы выявления, фиксации, изъятия, хранения, исследования, оценки цифровых следов;

4. как эти источники использовались в доказывании;

5. исследовать тактику производства конкретных следственных действий, особенно, не типичных;

6. какие и как в следственных действиях применялись тактические приемы;

7. выявить тактические комбинации и операции;

8. в каких следственных действиях имелись сложности, были допущены ошибки, упущения, какие из них по уголовным делам более типичны;

9. какие были удачные тактические решения;

10. анализ применения криминалистической тактики судом и гособвинителем;

11. особенности тактики защиты;

12. какие у Вас в связи с проведенным анализом уголовных дел имеются предложения, рекомендации...

Практику можно изучить на сайтах:

https://sud-praktika.ru/precedent/category/299.html

https://sudact.ru

https://sudrf.ru/

и иных.

Образец оформления сноски на судебную практику:

Приговор Якутского городского суда Республики Саха (Якутия) от 26.08.2019 № 1-681/2019 по делу № 1-1462/2018 // https://sudact.ru/regular/doc/8jIATe7oVfNK/ (дата обращения:…)

Уголовное дело 1-329/2013 // Архив Центрального районного суда г. Барнаула. // https://... (дата обращения: …)

Необходимо добавлять ссылку на сайт, откуда была взята практика.

Студентам, проходящим практику на кафедре, рекомендуется ***за неделю до ее окончания прикрепить проект отчета*** *на сайт https://portal.edu.asu.ru/course/view.php?id=8570, чтобы было время устранить возможные недостатки.*

3) Проекты процессуальных документов (3 шт.). Не должны содержать персональные данные.

ГЛАВА 4. ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ КОНТРОЛЯ ЗНАНИЙ

4.1. ПРИМЕРЫ ЗАДАНИЙ ЗАКРЫТОГО ТИПА

В заданиях этого типа имеются различные варианты ответа на поставленный вопрос: из ряда предлагаемых выбираются один или несколько правильных ответов, выбираются правильные (или неправильные) элементы списка.

1. Из каких источников могут поступать данные о личности компьютерных преступников?

1. сведения, полученные в ходе производства следственных действий;
2. сведения из СМИ;
3. сведения, полученные в результате ОРД;
4. сведения из показаний свидетелей;
5. из рассказов очевидцев;
6. ***все ответы верные.***

Ответ: 6.

2. Какие жаргонизмы широко используется в отношении преступников в литературе и средствах массовой информации?

1. ***хакеры;***
2. ***кардеры;***
3. ***крэкеры;***
4. джокеры;
5. докеры.

Ответ: 1, 2, 3.

3. Выберите из перечисленного, что обычно является мотивом преступных действий несовершеннолетних киберпреступников?

1. исследовательский интерес, самоутверждение, жажда славы;

2. корыстные побуждения, политические побуждения, игровой интерес;

3. жажда наживы, месть, игровой интерес;

4. из предложенных вариантов нет верного ответа.

Ответ: 1.

4. Лица какого пола чаще всего совершают компьютерные преступления?

1. мужского

2. женского

3. все вышеперечисленное.

Ответ: 1.

5. Какие факторы способствуют противоправной деятельности компьютерных преступников и влияют на низкую раскрываемость таких дел?

1. большое количество совершаемых эпизодов преступлений;

2. технологии анонимизации пользователей информационных сетей;

3. низкая юридическая осведомленность в сфере компьютерных преступлений;

4. низкий уровень знаний в области информационной безопасности у населения;

5. сложность получения цифровой информации.

6. ***все ответы верные.***

Ответ: 6.

6. Какое неотложное следственное действие является наиболее значимым по компьютерным преступлениям?

1. осмотр места происшествия;

2. получение информации о соединениях между абонентами и (или) абонентскими устройствами;

3. допрос;

4. обыск;

5. наведение справок;

6. получение компьютерной информации.

Ответ: 1.

7. Родовым объектом преступлений в сфере компьютерной информации является?

1. экономическая безопасность;

2. отношения в сфере охраны авторского права;

3. информационная безопасность;

4. общественные отношения, которые возникают в связи с поддержанием общественного порядка и обеспечением общественной безопасности.

Ответ: 4.

8. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе по сети Интернет?

1. аутентификация;

2. авторизация;

3. экспертиза;

4. шифрование.

Ответ: 4.

9. При расследовании преступлений в сфере компьютерной информации какие обстоятельства подлежат выявлению?

1. способ совершения преступлений;
2. характер и размер причиненного вреда;
3. время совершения преступления;
4. место совершения преступления;
5. обстоятельства, способствовавшие совершению преступления;
6. ***все ответы правильные.***

Ответ: 6.

10. Предметом преступного посягательства в сфере компьютерной информации является?

1. компьютер;
2. ***программное обеспечение компьютера;***
3. флешка или CD-диск.

Ответ: 2.

11. Субъектом преступлений в сфере компьютерной информации является:

1. юридическое или физическое лицо, не имеющие разрешения для работы с информацией определенной категории;
2. ***физическое вменяемое лицо, достигшее 16-летнего возраста;***
3. физическое вменяемое лицо, достигшее 18-летнего возраста;
4. физическое вменяемое лицо, достигшее 14-летнего возраста.

Ответ: 2.

12. Выберите проблемы, связанные с расследованиеи преступлений в сфере компьютерной информации:

1. недостаточная эффективность криминалистических методик в расследовании;
2. недостаточность обобщения судебно-следственной практики;

3. недостаточный уровень подготовки сотрудников следственных органов;

4. все варианты правильны.

Ответ: 4.

13. Специфика электронно-цифровых следов проявляется в том, что:

1. их легко обнаружить;
2. их можно увидеть не вооруженным глазом на экране монитора компьютера;
3. могут быть легко сокрыты и уничтожены;
4. могут быть легко инсценированы;
5. у таких следов нет специфики.

Ответ: 4, 5.

14. Криминалистическая характеристика преступлений в сфере компьютерной затрагивает информацию о:

1. направленности первоначальных следственных действий;
2. ***образовании преступника;***
3. ***средствах информационной безопасности потерпевших;***
4. производстве судебной компьютерно-технической экспертизы.

Ответ: 2, 3.

15. Перечислите виды компьютерных преступлений:

1. изменение компьютерных данных;
2. компьютерное мошенничество;
3. компьютерное пиратство;
4. получение конфиденциальных сведений с экрана монитора;
5. ***все ответы верные.***

Ответ: 5.

16. Согласно УК РФ к компьютерной информации относятся:

1. информационные ресурсы (базы данных, текстовые, графические файлы и т.д.), представленные в форме электрических сигналов;

2. программы, обеспечивающие функционирование компьютера или информационно-телекоммуникационных сетей, хранение, обработку и передачу данных;

3. информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ;

4. все ответы правильные.

Ответ: 3.

17. Под определение высокотехнологичного преступления в большей степени подходит:

1. преступление, совершаемое в групповой форме полноструктурным способом с помощью специально созданных или модифицированных программных, программно-аппаратных или аппаратных средств с использованием информационных сетей, в результате чего наносится значительный вред чьим-либо интересам или же возникает реальная угроза его наступления;

2. преступление, совершаемое в групповой форме полноструктурным способом оригинальными средствами с использованием информационных сетей, что объективно предопределяет криминалистические сложности расследования;

3. любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу компьютерной информации;

4. распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации (клеветы, материалов

порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду, и т. п.), неправомерный доступ к компьютерной информации, в том числе входящую в критическую информационную инфраструктуру государства.

Ответ: 1.

18. Кто чаще всего совершает высокотехнологичные преступления?

1. молодые люди;
2. специалисты в области компьютерной техники и информации;
3. программисты;
4. все перечисленные;
5. ***организованные группы лиц, состоящие из не специалистов и специалистов в области компьютерной информации.***

Ответ: 5.

19. С помощью каких средств совершаются преступления в сфере компьютерной информации?

1. персональный компьютер, ноутбук, смартфон;
2. фотоаппарат, видеокамера, бинокль;
3. ***любых средств компьютерной техники.***
4. любых технических средств.

Ответ: 3.

20. Предметом преступлений в сфере компьютерной информации является:

1. ЭВМ как средство совершения преступления;
2. Компьютеры и программное обеспечение;
3. информация на машинном носителе;
4. ***компьютерная информация на любом носителе.***

Ответ: 4.

21. Криминалистический аспект организации расследования компьютерных преступлений в большей степени связан с:

1. познанием закономерностей, характеризующих деятельность следователя (дознавателя), направленную на упорядочение индивидуальной деятельности по организации расследования компьютерных преступлений;

2. взаимодействием при раскрытии и **расследовании компьютерных** ***преступлений участвующими в них субъектами;***

3. с подготовкой процессуального документа.

Ответ: 2.

22. Криминалистика включает в себя прогнозирование в качестве:

1. составного элемента научного познания;

2. детального элемента научного познания;

3. обособленного элемента научного познания;

4. дополнительного элемент научного познания.

Ответ: 1.

23. Характерные черты криминалистического прогнозирования:

1. деятельность носящая научный характер;

2. деятельность носящая соцаильно-ориентированный характер;

3. прогностическая деятельность непосредственно связана с познанием настоящего состояния субъекта;

4. прогностическая деятельность непосредственно связана с познанием настоящего состояния объекта.

Ответ: 1.

24. Технология, нацеленная на выявление криминальной активности в сети Интернет это?

1. honeypot;

2. honeycot;

3. hony;

4. honeytop.

Ответ: 1.

25. Кто не является субъектом криминалистического предупреждения компьютерных преступлений это?

1. дознаватели;
2. сотрудники оперативно-розыскных органов;
3. судьи;
4. прокуроры;
5. ***адвокаты.***

Ответ: 5.

26. Роль работников прокуратуры в системе криминалистического предупреждения компьютерных преступлений определяется:

1. вынесением актов прокурорского реагирования;
2. поддержание гособвинения в суде;
3. оба варианта верны;
4. все варианта неверны.

Ответ: 1.

27. Какое из перечисленных следственных действий не является типичным для расследования преступлений в сфере компьютерной информации?

1. выемка и осмотр предметов и документов;
2. допрос свидетелей;
3. ***следственный эксперимент и проверка показаний на месте.***

Ответ: 3.

28. Для эффективного расследования преступлений в сфере компьютерной информации необходимо:

1. повышение заработной платы следователей и оперативных работников;

2. повышение количества следователей, оперативных работников в области компьютерной информации;

3. привлечение специалистов для помощи органам, осуществляющим расследование преступлений.

4. все варианты правильные.

Ответ: 1.

29. В настоящее время проблематичным является то обстоятельство, что получение доказательств по большинству преступлений в сфере компьютерной информации невозможно без соответствующих программно-аппаратных средств, которыми зачастую не обладают правоохранительные органы по причине их:

1. ненадобности;
2. высокой стоимости;
3. малой распространенностью;
4. сложностей освоения.

Ответ: 2.

30. При расследовании преступлений в сфере компьютерной информации доказыванию не подлежит:

1. способ совершения преступления;
2. характер и размер причиненного вреда;
3. кто имеет доступ к информации содержащейся в ЭВМ;
4. все варианты правильные.

Ответ: 3.

4.2. ПРИМЕРЫ ЗАДАНИЙ ОТКРЫТОГО ТИПА

В заданиях этого типа не дается набор готовых ответов для выбора, требуется самостоятельный творческий ответ.

1. Мерами предупреждения компьютерных преступлений являются:

- технические;
- организационные;
- правовые;
- методические.

2. Перечислите элементы полноструктурного способа совершения преступлений в сфере компьютерной информации:

- подготовка;
- совершение;
- сокрытие.

3. Наиболее распространенным мессенджером, используемым в России для вербовки в международные экстремистские и террористические организации, является:

- "Telegram".

4. Какие факторы способствует противоправной деятельности преступников?

- низкий уровень прикладного программного обеспечения;
- наличие и состояние средств защиты компьютерной информации;
- недостаточный уровень квалификации правоохранительных органов в области расследования преступлений;
- технологии анонимизации пользователей информационных сетей;
- недостаточная юридическая и техническая грамотность населения.

5. Задачами деятельности террористов в сети Интернет часто являются;

- пропаганда террористической идеологии и вербовка в террористические организации.

6. Какие элементы криминалистической характеристики преступлений в сфере компьютерной информации являются важнейшими?

- предмет преступного посягательства;
- способ совершения преступления;
- характеристика личности преступника и потерпевшего;
- обстановка преступления;
- средства преступления;
- следовая картина преступления;
- причины и условия, способствующие совершению преступления.

7. Целью фишинга является?

- получение чужих личных данных.

8. Как в криминалистике принято называть следы компьютерных преступлений?

- электронно-цифровые следы;
- виртуальные следы.

9. Основные субъекты криминалистического предупреждения компьютерных преступлений?

- оперативные сотрудники;
- следователи;
- дознаватели;
- судьи;
- прокуроры.

10. Какие основные обстоятельства, возникающие у следствия в расследовании преступлений, совершенных с удаленно расположенного от объекта преступного посягательства компьютера, вызывают криминалистические сложности?

- установление принадлежности следов конкретному лицу;
- установление места совершения преступления;
- установление размера ущерба;
- доказывание групповой формы совершения преступления и установление организаторов преступной деятельности;
- установление всех эпизодов преступной деятельности;
- установление средств преступления.

11. Что необходимо для осуществления высокотехнологичного преступления?

- использование информационно-телекоммуникационных технологий;
- оригинальные или модифицированные компьютерные средства;
- подготовка к преступлению и его сокрытие, а также противодействие расследованию;
- групповой состав;
- специальные технические знания у преступников.

12. Что такое IP-адрес?

- это уникальный идентификатор устройства в компьютерной сети.

13. В чём заключается задача анонимайзера?

- в сокрытии компьютерных данных.

14. Следовая картина – это?

- элемент криминалистической характеристики преступления;
- совокупность следов, характерных для определенных преступлений.

15. В следовая картину неправомерного удаленного доступа к компьютерной информации входят следы, оставляемые в?

- компьютерной технике преступника;
- компьютерной технике потерпевшего;
- компьютерной технике провайдера, а также шлюзах, маршрутизаторах, коммуникаторах и подобной технике, через которую проходит компьютерная информация.

16. Наиболее распространенными следственными действиями по компьютерным преступлениям являются?

- следственный осмотр;
- обыск и выемка;
- допрос;
- судебная компьютерно-техническая экспертиза.

17. Согласно позиции, высказанной В.А. Мещеряковым, эти следы, связанные с изменением состояния автоматизированной системы называются:

- виртуальными.

18. В.Б. Вехов предлагает ввести в криминалистический категориальный аппарат новое понятие как:

- электронно-цифровой след.

19. Какая идентификационно-справочная информация может быть обнаружена на сервере провайдера;

- информация о фамилии, имени, отчества.

20. Причины возможного длительного расследования компьютерного преступления?

- скрытость информации;
- анонимность в интернете;

- анализ больших данных;

- недостаточность материально-технической базы, прежде всего, программного обеспечения по компьютерной криминалистике;

- противодействие расследованию;

- необходимость выявления и сбора электронно-цифровых следов.

ЗАКЛЮЧЕНИЕ

Содержавшаяся в учебном пособии теоретическая часть формирует у обучающихся необходимые знания по основам противодействия компьютерным преступлениям, представления о криминалистической характеристике данных преступлений, а также способствует проведению криминалистического доказывания совершения таких преступлений.

Выполнение заданий, предложенных в настоящем учебном пособии, обеспечит формированию системы знаний, повышающих возможности избрания правильной линии поведения, тактически верных решений и действий в различных криминалистических ситуациях расследования компьютерных преступлений. Это становится возможным за счет совершенствования имеющихся и получения обучающимися новых компетенций, формируемых из знания о современных угрозах со стороны киберпреступности, использующей информационно-коммуникационные технологии, теории и практики расследования таких преступлений, навыков сбора эмпирических и иных данных для проведения самостоятельного научного исследования, а также развития практикоориентированных умений и навыков эффективного противодействия компьютерной преступности.

Использование предложенных в пособие заданий способствует повышению эффективности педагогического процесса, позволяющего направить обучающихся по рациональным путям самостоятельной работы, помочь в осуществлении контроля знаний обучающихся, а также организовать работу в дистанционном формате.

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

28. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114 - 116.

29. 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.

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

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

32. 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.

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

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

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

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

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

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

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

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

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

42. Поляков В.В. Система honeypot как инструмент сбора информации для противодействия киберпреступности // Библиотека криминалиста : научный журнал. – 2017. – №1 (30). – С. 250-254.

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

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

45. 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.

46. Сафронов А.Ю., Поляков В.В. Проблемы юридического и лингвистического определения фальсификации доказательств в уголовном судопроизводстве // Юрислингвистика. – 2019. – № 12. – С. 13-17.

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

48. 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.

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

50. 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.

ПРИЛОЖЕНИЕ 1

Примерная анкета для опроса специалистов, участвующих в противодействии компьютерным преступлениям

Уважаемый коллега!

Просим Вас ответить на следующие вопросы

1.1. Вы работаете:

□ в органах прокуратуры

□ в органах МВД

□ в органах Следственного комитета

□ в органах ФСБ

□ в суде

□ в адвокатуре

□ в экспертном учреждении

□ в государственном учреждении

□ в коммерческой организации

1.2. Ваш стаж работы:

□ до 2 лет

□ до 5 лет

□ до 10 лет

□ до 20 лет и свыше

1.3. Ваше образование:

□ высшее юридическое

□ высшее гуманитарное

□ высшее техническое

□ высшее естественно-научное

□ среднее специальное

1.4. Вы считали бы полезным дополнительное обучение в области расследования компьютерных преступлений и прохождение:

□ переподготовки

□ повышения квалификации

□ не требуется

2.1. Вы имели опыт расследования и реагирования на компьютерное преступление (правонарушение):

□ да

□ нет

2.2. Ваша оценка уровня выявляемости компьютерных преступлений:

□ высокий (регистрируется свыше 50% реально совершенных преступлений)

□ средний (регистрируется примерно от 20 до 50% реально совершенных преступлений)

□ низкий (регистрируется менее 20% реально совершенных преступлений)

2.3. Ваша оценка раскрываемости зарегистрированных компьютерных преступлений:

□ раскрываемость высокая

□ раскрываемость удовлетворительная

□ раскрываемость низкая

3.1. В совершении компьютерных преступлений (правонарушений), с которыми вы сталкивались, участвовали:

□ одно лицо

□ группа лиц

□ организованная группа

□ преступное софобщество

3.2. При совершении преступления использовались:

□ сеть Интернет

□ вредоносное программное обеспечение

□ специально созданные или модифицированные программно-аппаратные устройства

□ специально созданные или модифицированные технические устройства

□ методы обмана и манипулирования людьми (социальная инженерия)

3.3. Имелась ли подготовка и сокрытие компьютерных преступлений:

□ имелась подготовка

□ имелось сокрытие

□ не имелось

3.4. Имело ли место противодействие расследованию компьютерных преступлений (правонарушений) со стороны:

□ подозреваемых (обвиняемых)

□ связанных с подозреваемыми (обвиняемыми) лиц

□ защитников

□ свидетелей

□ потерпевших граждан и

□ потерпевших юридических лиц

3.5. Имелась ли при расследовании компьютерных преступлений потребность в привлечении специалиста в сфере компьютерных технологий:

□ да

□ нет

4.1. Какие обстоятельства в первую очередь способствовали совершению компьютерных преступлений:

□ низкий уровень защищенности компьютерной техники

□ соучастие в преступлении лиц, имевших доступ к компьютерной технике

□ недостаточная подготовка и халатность сотрудников, использующих компьютерную технику;

□ другие обстоятельства (просьба указать)

_____

4.2. Какие обстоятельства в первую очередь затрудняли расследование компьютерного преступления:

□ высокая сложность расследования

□ сокрытие преступниками следов преступления

□ противодействие расследованию

□ несвоевременность выявления преступления

□ сложность выявления, фиксации, изъятия, исследования и оценки электронно-цифровых следов

□ нехватка специалистов и экспертов

□ нехватка оборудования, необходимого при производстве следственных действий

□ сложность доказывания групповой формы совершения преступления

□ сложность установления и доказывания размера причиненного преступлением ущерба

□ трансрегиональность или трансграничность преступления

□ многоэпизодность преступления

□ многообъектность преступления

□ несовершенство методической базы (недостаточность эффективных методик расследования и практических рекомендаций и т.д.)

□ несовершенство уголовного законодательства

□ несовершенство уголовно-процессуального законодательства

□ другие обстоятельства (просьба указать)

_____

4.3. Какие меры в первую очередь способствовали бы предупреждению компьютерных преступлений:

□ правовые (совершенствование нормативной базы)

□ организационные

□ методические (разработка методик и рекомендаций)

□ технические

□ другие (просьба указать)

_____

5. Замечания, пояснения, пожелания (по Вашему усмотрению**)**

_____

Спасибо за Вашу помощь в исследовании!

ПРИЛОЖЕНИЕ 2

Словарь основных понятий и терминов, применяемых при расследовании компьютерных преступлений.

А

Адаптер — приспособление, устройство или деталь, предназначенные для соединения устройств, не имеющих непосредственного способа соединения, связи компьютера с периферийными устройствами.

Адрес — символ или группа символов, которые идентифицируют регистр, отдельные части памяти или некоторые другие источники данных, либо место назначения информации.

Алгоритм — это совокупность точно заданных правил решения некоторого класса задач или набор инструкций, описывающих порядок действий исполнителя для решения определенной задачи.

Антивирусные программы — специальные программы, разработанные для обнаружения, удаления и защиты от компьютерных вирусов.

Арифметико-логическое устройство — блок процессора, который под управлением устройства управления служит для выполнения арифметических и логических преобразований (начиная от элементарных) над данными, называемыми в этом случае операндами. Разрядность операндов обычно называют размером или длиной машинного слова.

Архитектура компьютера — логическая организация, структура и ресурсы компьютера, которые может использовать программист. Определяет принципы действия, информационные связи и взаимное соединение основных логических узлов компьютера.

Аски (ASCII) — 7-битовый код, который долгое время служил международным стандартом и лежит в основе многих современных стандартов кодирования текста.

Б

База данных — совокупность данных, которая включает в себя определенные правила, принципы хранения, описания и управления данными.

Байт — единица хранения и обработки цифровой информации, совокупность битов, обрабатываемая компьютером одновременно.

Библиотека стандартных подпрограмм — совокупность подпрограмм, составленных на одном из языков программирования и удовлетворяющих единым требованиям к структуре, организации их входов и выходов, описаниям подпрограмм.

Бит — это минимальная единица измерения количества информации, принимающая значения "0" или "1".

Блокирование — это совершение действий, приводящих к ограничению или закрытию правомерного доступа к компьютерной информации и не связанных с ее уничтожением.

В

Ввод — взаимодействие между обработчиком информации (например, компьютер) и внешним миром, который может представлять как человек (субъект), так и любая другая система обработки информации. Сигнал или данные, полученные системой.

Веб-программирование — раздел программирования, ориентированный на разработку веб-приложений (программ, обеспечивающих функционирование динамических сайтов Всемирной паутины).

Веб-сервис, веб-служба (Web service) — идентифицируемая уникальным веб-адресом (URL-адресом) программная система со стандартизированными интерфейсами.

Веб-сайт, интернет-сайт (Web site) — основной вид ресурсов всемирной паутины, представляющей собой совокупность веб-страниц, созданных на основе языка разметки HTML и объединенных общим доменным

именем. Сайт размещается на веб-сервере, который является узлом глобальной компьютерной сети интернет.

Видео-конференц-связь (ВКС) — способ осуществления процессуальных действий, предусмотренных законом, с использованием программно-технических средств передачи аудио- и видеоинформации по каналам связи с одним или несколькими абонентами.

Вирус компьютерный — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

Внешняя память — место длительного хранения данных (программ, результатов расчетов, текстов и т. д.), не используемых в настоящий момент в оперативной памяти.

Вывод — обратный процесс, когда данные передаются после обработки из памяти компьютера на внешний носитель (экран монитора, принтер и другие устройства).

Г

Графический редактор — программа или комплекс программ, позволяющих создавать и редактировать изображения на экране компьютера: рисовать линии, раскрашивать области экрана, создавать надписи различными шрифтами, обрабатывать изображения, полученные с помощью сканеров. Некоторые редакторы обеспечивают возможность получения изображений трехмерных объектов, их сечений и разворотов.

Д

Дистанционные технологии — технологии, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии участников.

Доверенная среда — созданное комплексом технических и организационных мер пространство, которое обеспечивает его участникам

предсказуемый результат взаимодействий, при этом степень доверенности среды определяется надежностью информации в ней.

Документ — материальный носитель с зафиксированной на нем информацией в виде текста, звукозаписи (фонограммы), изображения или их сочетания, предназначенный для передачи во времени и пространстве в целях общественного использования и хранения.

Документооборот — движение документов с момента их создания или получения до завершения исполнения, помещения в дело и (или) отправки.

Дисковод — устройство компьютера, позволяющее осуществить чтение и запись информации на съемный носитель информации.

Драйверы — программное обеспечение, с помощью которого другое программное обеспечение (операционная система) получает расширяющие возможности по управлению аппаратными устройствами.

Е

Единая биометрическая система — государственная информационная система, обеспечивающая сбор биометрических персональных данных, их хранение и использование для аутентификации и идентификации пользователя.

Единая система идентификации и аутентификации — федеральная государственная информационная система, предназначенная для формирования единых методов регистрации, идентификации и аутентификации пользователей во всех государственных информационных системах, цель которой упорядочить и централизовать процессы регистрации, идентификации, аутентификации и авторизации пользователей.

Единый портал государственных и муниципальных услуг — государственная информационная система, обеспечивающая предоставление государственных и муниципальных услуг в электронной форме, а также доступ заявителей к сведениям о государственных и муниципальных услугах, предназначенным для распространения с использованием информационно-

телекоммуникационной сети «Интернет» и размещенным в государственных и муниципальных информационных системах, обеспечивающих ведение реестров государственных и муниципальных услуг.

И

Идентификатор — уникальный признак объекта, позволяющий отличать его от других объектов, то есть идентифицировать.

Инструментальные программные средства — программы, которые используются в ходе разработки, корректировки или развития других прикладных или системных программ. По своему назначению они близки системам программирования.

Интегрированные пакеты программ — набор взаимосвязанных прикладных программ, ориентированных на решение комплекса задач и поддерживающих единый способ взаимодействия пользователя со всеми программами из пакета, а также единый способ представления данных. Обычно такие пакеты включают в себя текстовый редактор, табличный процессор, СУБД, пакет графического отображения данных и телекоммуникационную программу.

Интернет — коммуникационная сеть и всемирная система объединенных компьютерных сетей для хранения и передачи информации.

Интерпретация — построчный анализ, обработка и выполнение исходного кода программы или запроса, в отличие от компиляции, где весь текст программы перед запуском анализируется и транслируется в машинный или байт-код без ее выполнения.

Интерфейс — общая граница между двумя функциональными объектами, требования к которой определяются стандартом; совокупность средств, методов и правил взаимодействия (управления, контроля и т.д.) между элементами системы.

Информатизация — организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и

использования информационных ресурсов и реализации информационных отношений.

Информационное пространство — совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

Информационная технология — совокупность методов, программно-технических и технологических средств, обеспечивающих сбор, накопление, обработку, хранение, представление и распространение информации, а также автоматизацию управления бизнес-процессами организаций, проектирования и производства различного оборудования.

Информационно-поисковая система (ИПС) — система, обеспечивающая поиск и отбор необходимых данных в специальной базе с описаниями источников информации (индексе) на основе информационно-поискового языка и соответствующих правил поиска.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информация — сообщение или сигнал, совокупность данных, сведения, рассматриваемые в контексте их содержания, структурной организации, динамики (процессов создания, передачи, восприятия, использования, репрезентирования, анализа, хранения и т.п.).

К

Канал связи — материальная среда, а также физический или иной процесс, посредством которого осуществляется передача сообщения, то есть распространение сигналов в пространстве с течением времени.

Клиент (рабочая станция) — компьютер, пользующийся ресурсами сети.

Ключевое слово — слово в тексте, которое в совокупности с другими ключевыми словами дает высокоуровневое описание содержания текстового документа, выявляет его тематику.

Команда — предписание о выполнении отдельного законченного действия.

Компилятор — программа, которая переводит исходный код на языке программирования в машинный код.

Компрометация ключей — утрата доверия к используемым ключам, обеспечивающим безопасность информации, её целостность, конфиденциальность, подтверждение авторства.

Компьютер — устройство или система, способная автоматически выполнять заданную, изменяемую последовательность операций.

Компьютеризация — процесс широкого внедрения в практическую деятельность человека, в повседневный быт электронных устройств для автоматизированной обработки информации — компьютеров.

Компьютерная информация — это сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, то есть .любая информация, которая может быть введена в компьютер или создана с помощью компьютера и использоваться для обработки, хранения, передачи и получения различных данных.

Компьютерный вирус — программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению.

Контроллер — электронное устройство, предназначенное для автоматического управления техническим объектом (процессом) по заданному алгоритму.

Конфиденциальная информация — сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих

распространению в средствах массовой информации в установленных федеральными законами случаях.

Копирование компьютерной информации — перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме.

Л

Линии связи — линии передачи, физические цепи и линейно-кабельные сооружения связи.

Лог-файл — своеобразный журнал событий, в котором в текстовом сокращенном виде автоматически записывается важная информация о работе системы или программы, например, сведения об ошибках, действиях пользователей и других событиях, которые происходят на сервере или в системе.

«Люк» - использование ошибки или неудачи в логике построения программы для несанкционированного доступа к данным путем встраивания определенного кода управляющей команды.

М

«Маскарад» — процесс несанкционированного проникновения в компьютерную сеть с использованием средств выдачи себя за законного пользователя.

Массив — структура данных, хранящая набор значений (элементов массива), идентифицируемых по индексу или набору индексов, принимающих целые (или приводимые к целым) значения из некоторого заданного непрерывного диапазона.

Массовая информация — предназначенные для неопределенного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Машинный язык — система команд (набор кодов операций) конкретной вычислительной машины, которая интерпретируется

непосредственно процессором или микропрограммами этой вычислительной машины.

Многоточечная видеоконференция — способ организации видеоконференцсвязи с несколькими участниками процесса, находящимися в разных (более двух) территориально удаленных местах.

Модификация информации — процесс изменения данных с целью внесения ошибок, искажений или вредоносных изменений. Причины модификации информации могут быть различными, включая финансовую выгоду, политические или личные мотивы. Виды модификации информации включают подделку, изменение или удаление данных. Последствия модификации информации могут быть серьезными, включая потерю доверия, финансовые потери или нарушение безопасности.

Н

Накопитель на жестких магнитных дисках — устройство хранения информации, основанное на принципе магнитной записи.

О

Оболочки — программа, предоставляющая интерфейс для взаимодействия пользователя с функциями системы.

Обработка информации — вся совокупность операций (сбор, ввод, запись, преобразование, считывание, хранение, уничтожение, регистрация), осуществляемых с помощью технических и программных средств, включая обмен по каналам передачи данных.

Оперативная память (ОЗУ) — в большинстве случаев энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором.

Оператор — команда, обозначающая определенное математическое или логическое действие, выполняемое с данными (операндами). Является минимальным автономным элементом компьютерной программы.

Операционная система — программное обеспечение, которое управляет компьютерами (включая микроконтроллеры) и позволяет запускать на них прикладные программы.

Отладка — поиск, анализ и устранение ошибок в программном обеспечении, которые были найдены во время тестирования.

П

Пакет — блок данных в сети передачи информации, который имеет определенную структуру, включающую заголовок и поля данных.

«Перехват информации» — это несанкционированное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

Подпрограмма — поименованная или иным образом идентифицированная часть компьютерной программы, содержащая описание определенного набора действий. Подпрограмма может быть многократно вызвана из разных частей программы. В языках программирования для оформления и использования подпрограмм существуют специальные синтаксические средства.

Пользователь информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Порты устройств — электронные схемы, содержащие один или несколько регистров ввода-вывода и позволяющие подключать периферийные устройства компьютера к внешним шинам микропроцессора.

Постоянная память (ПЗУ) — энергонезависимая память, используется для хранения данных.

Прикладная программа — обширный класс программ, предназначенный для решения отдельных определенных пользователем задач, связанных с обработкой данных в определенной области деятельности.

Протокол коммуникации — согласованный набор конкретных правил обмена информацией между разными устройствами передачи данных.

С

Сервер — компьютер для обслуживания поступающих от других компьютеров запросов (например, посредством вычислительной сети), а также программа, обеспечивающая управление доступом к сетевым ресурсам.

Сетевой адаптер — это устройство, обеспечивающее возможность связи компьютера с локальной сетью.

Сеть компьютерная — взаимосвязанные вычислительные устройства, которые могут обмениваться данными и совместно использовать ресурсы. Эти сетевые устройства используют систему правил, называемых коммуникационными протоколами.

Система программирования — комплекс из различного программного обеспечения, который применяют для создания, тестирования, отладки и оптимизации программного кода.

Система управления базами данных (СУБД) — совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных.

Системные программы — программы общего пользования, выполняемые вместе с прикладными и служащие для управления ресурсами компьютера — центральным процессором, памятью, вводом-выводом.

Средства электронной подписи — программно-аппаратное или только программное средство, предназначенное для создания ключевой пары, формирования и проверки электронной подписи на электронном документе.

Структурное программирование — разработка программ с помощью представления их в виде иерархической структуры блоков.

Т

Текстовый редактор — самостоятельная компьютерная программа или часть программного комплекса, которая предназначена для создания и редактирования текстовых данных.

Тестирование — проверка соответствия между реальным поведением программы и ее ожидаемым поведением.

Тип данных — набор или группировка значений данных, обычно задаваемых набором возможных значений, набором разрешенных операций над этими значениями и /или представлением этих значений в виде типов машин.

Топология компьютерной сети — физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

Транслятор — класс компьютерных программ, которые осуществляют преобразование символьной записи программ из одной формы в другую.

У

Уничтожение информации — приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления.

Ф

Файл — часть внешней памяти компьютера, имеющая идентификатор и содержащая данные.

Фильтр — совокупность параметров, на основании которых программой принимается решение пропускать пакет или заблокировать его.

Ц

Цикл — блок кода, который требуется выполнять много раз в процессе работы созданного приложения.

Цифровизация — процесс организации выполнения в цифровой среде функций и деятельности, ранее выполнявшихся людьми и организациями без использования цифровых продуктов.

Цифровое пространство — пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур на основе норм регулирования, механизмов организации, управления и использования.

Цифровой суверенитет — способность государства проводить (формировать и реализовывать) самостоятельный политический курс в цифровой сфере (отстаивать интересы, обеспечивать безопасность и т.д.) внутри страны и в международных отношениях.

Ч

Червь — программа, распространяющаяся по сети свои копии, используя уязвимости сетевых протоколов или сетевых программ.

Ш

Шифр — совокупность обратимых преобразований множества открытых текстов, заданных алгоритмом криптографического преобразования.

Шлюз — устройство, предназначенное для соединения двух локальных сетей. Перед передачей данных из одной сети в другую шлюзовой интерфейс их преобразует, обеспечивая совместимость протоколов.

Штриховой код (бар-код) — графическая информация, наносимая на поверхность, маркировку или упаковку изделий, предоставляющая возможность считывания ее техническими средствами.

Э

Электронный носитель — материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники.

Я

Язык ассемблера — это язык программирования, который часто используют, чтобы написать программы для аппаратных платформ или архитектур.

Язык высокого уровня — это язык программирования, разработанный для быстроты и удобства использования программистом.

Учебное издание

Поляков Виталий Викторович

МЕТОДИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ

Публикуется в авторской редакции

Оформление обложки *Ю.В. Луценко*

Издательская лицензия ЛР 020261 от 14.01.1997 г.

Подписано в печать 31.07.2024. Дата выхода в свет 07.08.2024.

Формат 60х84 1/16. Бумага офсетная.

Усл.-печ. л. 4,88. Тираж 50. Заказ 433.

Типография Алтайского государственного университета:

656049, Барнаул, ул. Димитрова, 66