Содержание:

ВВЕДЕНИЕ

Без сомнений можно утверждать, что в настоящее время киберпреступность является серьезной глобальной проблемой. Об этом свидетельствуют договоры, принимаемые международным сообществом, для борьбы с данным видом высокотехнологичных преступлений.

Компьютерная преступность зародилась вследствие активного развития компьютерных и информационных технологий. Их совершенствование приводит к росту компьютерной преступности. Следует отметить, что быстрое развитие подобного рода технологий также ведет к качественному изменению киберпреступлений.

Способы совершения компьютерных преступлений становятся более изобретательными. Преступники используют новейшие технические решения и модифицированное и программное обеспечение. По другую же сторону, техническое и программное обеспечение правоохранительных органов, расследующих киберпреступления, не совершенствуется годами. В частности, это приводит к тому, что вопрос о средствах совершения компьютерных преступлений всегда остается малоизученным. Все это, в совокупности, подчеркивает актуальность исследования в рамках данной выпускной квалификационной работы.

Составление исследователями и правоведами теоретических основ и разработка методов борьбы с компьютерными преступлениями всегда на шаг

позади стремительно растущих масштабов деятельности преступников. Как результат - высокая латентность компьютерных преступлений.

Термин «компьютерные преступления» употребляется наряду с термином «киберпреступления», их часто используют как синонимы. Наличие различных подходов к определению данных понятий вызывает множество дискуссий.

Согласно мнению большинства исследователей в сфере высоких технологий, понятие «киберпреступность» гораздо шире, чем «компьютерная преступность» - это преступность, связанная как с использованием компьютеров или компьютерных

данных, так и информационных технологий и глобальных сетей, а также специального программного обеспечения.

Целью данной работы является криминалистическая характеристика технологий совершения компьютерных преступлений, рассмотрение некоторых современных проблем борьбы с киберпреступностью. Для достижения данной цели, необходимо решить определенные задачи:

- провести анализ различных подходов к определению понятия «компьютерные преступления» (киберпреступления);

- провести анализ понятия средств совершения компьютерных преступлений» (киберпреступлений), а также изучить их классификацию и виды;

- дать криминалистическую характеристику средствам совершения киберпреступлений;

- изучить личность киберпреступника;

Исходными данными для разработки темы стали научные труды исследователей в сфере информационных технологий (IT).

Объект исследования в представленной работе - компьютерные преступления и технологии их совершения.

Предметом исследования является компьютерная информация, подвергающаяся преступным действиям.

Методологическая основа работы - диалектический метод научного исследования, на базе которого был использован метод логического осмысления - в изложении материала, при формулировке выводов, предложений и рекомендаций.

Структура работы. Данная работа состоит из введения, двух глав, заключения и списка использованной литературы.

Глава 1. Компьютерные преступления и компьютерная криминалистика.

1.1. Современные подходы к определению компьютерных преступлений

Мировое сообщество находится в постоянном поиске методов борьбы с киберпреступностью, а также в процессе выработки единой международной политики.

В условиях этой постоянной борьбы возникла компьютерная криминалистика - форензика.

Следует отметить, что в большинстве развитых стран как прикладная наука полноценно существует форензика: был издан ряд научных трудов, в университетах имеются кафедры и проводятся учебные курсы. Сотрудники правоохранительных служб при раскрытии компьютерных преступлений обязаны следовать официальным рекомендациям, составленным соответствующими специалистами.

В России форензика пока что находится в зачаточном состоянии. В то же время качественные характеристики российских компьютерных специалистов находятся на передовом уровне, не уступая развитым странам. Отечественные ученые и эксперты-криминалисты активно развивают данное направление.

Профессор Федотов Н.Н. дает следующее определение форензики: это прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств[1].

Компьютерная криминалистика (форензика) является прикладной наукой о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах.

В настоящее время мировым сообществом не выработаны единая терминология и подход к определению понятию «киберпреступность», которое употребляется наряду с понятием «компьютерная преступность».

Глобальная сеть нематериальна и не может быть сведена к физическому воплощению. Потому термин «компьютерная преступность» по своему смыслу

определяет суть преступлений, совершенных с помощью компьютера. Однако в настоящее время, само понятие «компьютер» в размыто, так как практически все мобильные телефоны имеют доступ во всемирную сеть Интернет. Так, например, развитие LTE (сеть четвертого поколения) позволяет получить доступ к глобальной сети с такой скоростью и качеством, что не только не уступает по возможностям подключению к сети Интернет с помощью обычного персонального компьютера, но, порой, и превышает их.

В мировой практике термин «киберпреступность» впервые появился во второй половине XX века. Первые подобные преступления были связаны с проникновением в компьютерные системы путем их повреждения и хищением данных.

С течением времени, и как следствие развития компьютерных и телекоммуникационных технологий, понятие «киберпреступность» изменялось, включая в себя все новые и новые преступления.

Традиционные формы компьютерных преступлений переходили в новые, такие как: компьютерное мошенничество, несанкционированный доступ к личным данным, незаконное использование программного обеспечения.

Современные тенденции развития киберпреступности продолжаются и в XXI веке. Общедоступность глобальной сети Интернет, простота в использовании, анонимность и высокая скорость передачи данных превратила локальные киберпреступления в транснациональную киберпреступность.

В зарубежной литературе и во многих официальных документах кроме/вместо «computer crime» также часто употребляется термин «cyber crime» - киберпреступность, киберпреступление. Определения этого термина разные, существуют широкие и узкие трактовки.

Некоторыми исследователями киберпреступность связывается с преступлениями, совершаемыми в различных информационных сетях. Так, по мнению А.В. Суслопарова термин «киберпреступность» оправдан, если мы говорим о совершении компьютерных преступлений в рамках компьютерной сети, в частности, сети Интернет[2].

С.В. Воронцов отмечает, что термин «киберпреступность» используется для определения преступности в виртуальном пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в локальных и глобальных сетях».

В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков считают, что «киберпреступность» - это любое преступление, совершенное с помощью компьютерной сети, т.е. любое преступление, совершенное в электронной среде.

И.Г. Чекунов включает в понятие «киберпреступности» компьютерные средства и мобильную (сотовую) технику. По его мнению «под киберпреступностью следует понимать совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных».

Высказана также точка зрения, согласно которой киберпреступность относят к преступлениям, совершаемым посредством компьютерной техники против различных прав и благ человека. Такой позиции придерживается В.А. Номоконов, который определяет киберпреступность как «родовое понятие, охватывающее как компьютерную преступность в узком значении этого слова (где компьютер является предметом, а информационная безопасность - объектом преступления), так и иные посягательства, где компьютеры используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности».

В свою очередь В. Д. Курушин и В. А. Минаев считают, что киберпреступления - это действия в Интернете, при которых компьютер является либо орудием, либо предметом криминальных посягательств в виртуальном пространстве.

С позиции И. М. Рассолова, киберпреступления - это общественно опасные деяния, совершаемые с применением средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете[3].

Стоит отметить, что существует и обобщенный подход. Так, мнению Т.Л. Тропиной, киберпреступность - это «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей или компьютерных данных».

Международное право двинулось по пути разделения понятий «киберпреступность» и «компьютерные преступления». Советом Европы была принята Конвенция о киберпреступности (ноябрь 2001 г.), в которой был

употреблен термин «киберпреступность» («cybercrime»), а не «компьютерные преступления» («computer crime»).

В 2013 году Управлением ООН по наркотикам и преступности был опубликован отчет, в котором было отмечено, что понятие «киберпреступность» зависит от контекста и цели его употребления. В этом же документе отмечается, что в рассматриваемое понятие включаются любые деяния, направленные на нелегальное извлечение прибыли и иная противозаконная деятельность в киберпространстве.

В Уголовном Кодексе содержится состоящая из трех статей (272-274) глава «Преступления в сфере компьютерной информации». В соответствии с примечанием к ст. 272 УК «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

То есть под преступлениями в сфере компьютерной информации следует понимать общественно опасные деяния (предусмотренные главой 28 Раздела IX УК РФ), которые посягают на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Термин же «компьютерные преступления» несколько шире, чем «преступления в сфере компьютерной информации». Он охватывает и те преступления, где компьютерная техника, программы, компьютерная информация и цифровые каналы связи являются орудиями совершения преступления (понятно, что из разряда компьютерных преступлений мы исключаем такие преступления, в которых компьютерная техника используется лишь как материальная ценность) или объектом посягательства. К таким преступлениям относятся: мошенничество с применением банковских карт (кардинг), мошенничество с выманиванием персональных данных (фишинг), незаконное пользование услугами связи и иной обман в области услуг связи, промышленный и иной шпионаж, когда объектом являются информационные системы, и т.д.

По мнению Н.Н. Федотова компьютер и компьютерная информация могут играть три роли в преступлениях, которые автор относит к компьютерным:

• объект посягательства;

• орудие совершения;

• доказательство или источник доказательств .

Во всех трех случаях требуются специальные знания и специальные методы для обнаружения, сбора, фиксации и исследования доказательств.

В различных источниках имеется несколько определений «компьютерного преступления» - от самого узкого (только три вышеупомянутых состава) до самого широкого (все дела, касающиеся компьютеров). В форензике не требуется четкого определения компьютерного преступления. Форензика как бы сама есть определение. Компьютерным, с точки зрения форензики, можно называть любое преступление, для раскрытия которого используются методы компьютерной криминалистики.

1.2. Виды компьютерных преступлений

Основаниями для выделения различных видов киберпреступлений могут выступать: объект преступления, предмет преступного посягательства, способ совершения, мотив, тяжесть последствий совершенного преступления, и так далее. Мы рассмотрим наиболее распространенные классификации, предложенные исследователями в сфере компьютерной безопасности, а также изложенные в международных документах.

Некоторыми авторами производится разделение киберпреступлений на группы по объекту посягательства[4]:

А) преступления против конфиденциальной информации;

Б) целостности и доступности данных и компьютерных сетей;

В) экономические киберпреступления;

Г) против личных прав и неприкосновенности частной сферы;

Д) против общественных и государственных интересов.

Ю.М. Батуриным была предложена уголовно-правовая классификация компьютерных преступлений по способу их совершения и получила широкое распространение. Основой предложенной им классификации является кодификатор Международной уголовной полиции «Интерпол», который содержится в документе «Руководство Интерпола в компьютерной преступности».

Все киберпреступления, которые в документе обозначаются буквой «Q». Также имеется дополнительный идентификатор для обозначения определенной группы преступлений. Всего выделяется шесть групп:

1. Несанкционированный доступ или перехват (QA).

Неправомерный доступ к компьютерной системе или сети путем нарушения систем охраны.

Несанкционированный перехват - неправомерный и осуществленный с помощью технических средств перехват сообщений, приходящих в компьютерную систему или сеть, исходящих из компьютерной системы или сети и передаваемых в рамках компьютерной системы или сети.

2. Изменение компьютерных данных (QD).

Изменение компьютерных данных - неправомерное изменение данных с использованием вредоносного программного обеспечения.

3. Компьютерное мошенничество (QF).

Компьютерное мошенничество - введение, удаление или изменение компьютерных данных или программ, либо иное вмешательство в процесс обработки данных, с намерением получить незаконным путем экономическую выгоду. Может осуществляться с целью хищения и последующего использования данной информации или же ради развлечения.

Существует множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, использование фишинговых ссылок и т.д.

4. Незаконное копирование - «пиратство» (QR).

Незаконное копирование - «пиратство» - несанкционированное копирование программного обеспечения и иных форм интеллектуальной собственности.

5. Компьютерный саботаж (QS).

Компьютерный саботаж - введение, удаление или изменение компьютерных данных или программ с целью воспрепятствовать нормальному функционированию

компьютера или сети.

6. Прочие компьютерные преступления (QZ)

В данную подгруппу внесены такие киберпреступления, как: хищение информации, составляющей коммерческую тайну, передача конфиденциальной информации и прочие.

В настоящее время наиболее распространена классификация киберпреступлений, основанная на Конвенции Совета Европы о киберпреступности.

Согласно первоначальным документам киберпреступления подразделялись на четыре группы, в дальнейшем был принят дополнительный протокол, в соответствии с которым появилась пятая группа.

Первая группа это киберпреступления против конфиденциальности, целостности и доступности компьютерных данных и систем, такие как незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему.

Во вторую группу входят преступления, связанные с использованием компьютера, как средства совершения преступлений - а именно, как средство манипуляций с информацией. В эту группу входят компьютерное мошенничество и компьютерный подлог.

Третью группу составляют преступления, связанные с контентом, то есть с содержанием данных, размещенных в компьютерных сетях. Самый распространенный и наказуемый практически во всех государствах вид этих киберпреступлений - преступления, связанные с детской порнографией.

В четвертую группу вошли преступления, связанные с нарушением авторского права и смежных прав.

Пятая группа преступлений зафиксирована в отдельном протоколе - это акты расизма и ксенофобии, совершенные посредством компьютерных сетей.

Анализируя изложенный материал, следует отметить, что перечень компьютерных преступлений будет расширяться, так как существует тесная взаимосвязь между научно-техническим процессом и криминализацией новых видов киберпреступлений.

Работы исследователей внесли определенный вклад в изучение проблем киберпреступлений и кибербезопасности, однако эти работы можно считать по большей части устаревшими. Так, например, возможности Интернет - банкинга в настоящее время гораздо шире, чем несколько лет назад. Важнейшим основанием для дальнейшего исследования проблем киберпреступности также являются и произошедшие изменения гл. 28 УК РФ, регулирующей вопросы преступности в сфере компьютерной информации. Поэтому на современном этапе следует предпринять дополнительные шаги к изучению проблем киберпреступлений и их уголовно-правовой классификации (типологии).

Проведенный И.Г. Чекуновым анализ, позволяющий осуществить их классификацию по способам, средствам, целям, географии, по объектам и субъектам совершения преступлений, показывает, что характерными чертами киберпреступлений являются[5]:

1) киберпреступления совершаются особыми способами и средствами: с помощью компьютерной техники, ее соответствующего программного обеспечения, систем и средств связи, в том числе мобильных (отметим, что распространенным, является мошенничество с использованием интернетбанкинга и мобильных систем связи);

2) противоправные деяния совершаются в особом и законодательно не урегулированном виртуальном киберпространстве, в частности:

- в его глобальных и трансграничных масштабах: при этом компьютеры и серверы, используемые злоумышленниками, могут находиться не в одном государстве и к тому же мигрировать, например, в случае распространения нелегального порно;

- в географических рамках двух и более государств (например, в рамках Прибалтийских стран);

- в национальных рамках одного государства или определенной его территории.

Глобализация киберпреступности возрастает с ростом количества и улучшением технических возможностей компьютеров, с развитием их программного обеспечения, с совершенствованием кибернавыков злоумышленников, а также с ростом амбициозности их криминальных целей.

Киберпреступления совершаются, как правило, скрытно, т.е. они относятся к категории неочевидных преступных деяний.

Действия злоумышленников могут иметь как длящийся, так и разовый (одномоментный) характер: продолжительные DDoS-атаки, распространение спама, создание бот-сети, работа порнотрекера могут идти от нескольких мгновений до многих суток, месяцев, лет, то есть пока у злоумышленников имеется возможность для достижения поставленной цели.

В ходе совершения преступления могут использоваться один, десятки, сотни и тысячи компьютеров, например, если в программное обеспечение компьютеров злоумышленниками внедрена и используется разветвленная бот-сеть.

Субъектом противоправного деяния, как правило, является специалист в области IT-технологий. Участниками (соучастниками) киберпреступлений являются не только хакеры-профессионалы, но и различного рода мошенники, вымогатели и т.д.

Классифицируя киберпреступления на основе различных характеризующих их особенностей, следует подчеркнуть, что:

- цели киберпреступников достигаются путем неправомерного использования информационных коммуникационных технологий (ИКТ), особенно сети Интернет, мобильных средств и систем связи;

- применение современных информационно-коммуникационных технологий для совершения преступления создает специфические проблемы по установлению злоумышленника, самого факта и географического места совершения противоправного деяния, поскольку информационнокоммуникационные ресурсы, используемые для правонарушения, могут находиться не только в одной или двух, но и во многих странах (отсюда - большая латентность);

- доказательства, касающиеся таких преступлений, могут сохраняться и передаваться, как правило, только по электронным сетям (в этой связи возникает сложность сбора и закрепления доказательств, проведения процессуальных действий, усложняется и решение проблемы латентности);

- преступления, как указывалось выше, зачастую совершаются для достижения корыстных финансовых целей, однако цели могут быть и политическими, и экономическими, и террористическими;

- возрастает и становится устойчивой тенденция к сплочению киберпреступности, все более принимающей групповой характер совершения таких деяний, причем

объединение злоумышленников происходит на добровольной основе.

Профессор Н.Н. Федотов выделяет такие виды компьютерных преступлений, как[6]:

• Онлайн мошенничество. Данная форма мошенничества развилась с появлением интернет-магазинов. Низкие затраты на организацию торговли (как денег, так и времени) и небольшие убытки привлекают злоумышленников к созданию сайтов с видимостью обычного торгового предприятия с последующим обманом потребителей. Мошенниками часто используются сайты фиктивных брачных агентств, где под различными предлогами потребителей убеждают внести денежную сумму, а также обманные сайты для пожертвований и так далее. Криминалистическая характеристика всех подобных преступлений одинакова и сводится к размещению в Сети ложной информации для последующего получения с жертвы денег и исчезновением из Сети.

• Клевета, оскорбления и экстремистские действия в сети. Данное преступление заключается в размещении на различных ресурсах Сети оскорбительных, клеветнических или экстремистских материалов.

• DoS-атаки. Это атака типа «отказ в обслуживании», которая приводит к блокировке информации, нарушению работы компьютера или компьютерной сети. DoS-атаки обычно разделяют на два типа: использующие какие-либо уязвимости в атакуемой системе и не использующие уязвимостей. Во втором случае целью атаки являются ресурсы системы (процессор, ОЗУ, пропускная способность канала).

На этапах DoS-атаки также может быть использовано вредоносное программное обеспечение и осуществлены и некоторые виды неправомерного доступа к информации (копирование, уничтожение информации).

• Дефейс. Данное преступление заключается в изменении внешнего вида веб-сайта жертвы, получив права администратора, либо под аккаунтом (личным кабинетом) законного пользователя. Чаще всего мотивами дефейса являются: политические, религиозные и иные идеологические мотивы, личная неприязнь либо стремление продемонстрировать собственную квалификацию.

• Распространение вредоносного программного обеспечения (ПО). Существует большое количество вредоносного ПО, целью которых является не только получение выгоды, но и нарушение работы компьютера и сети.

• Кардинг. Преступления, связанные с использованием поддельных банковских карт.

• Фишинг. Выманивание у потерпевших их конфиденциальных данных. Как правило, речь идет о номерах банковских карт, их пин-кодах, паролях к системе интернет-банкам так далее. Выманивание данных происходит при помощи подложных сообщений электронной почты и/или подложных вебсайтов. Например, в подложном сообщении указывается адрес фишингового сайта Сбербанк: https://sber-bank.ru.

• Нарушение авторских прав (в сети и в оффлайне). Незаконное изготовление, копирование либо размещение объектов интеллектуальной собственности на онлайн и оффлайн ресурсах без разрешения правообладателя. Яркими примерами являются изготовление и распространение контрафактных Dvd-дисков, торренты.

• Кибersквоттинг. Кибersквоттингом называется приобретение домена с целью недобросовестного использования, либо с целью не допустить его добросовестного использования другим лицом. В настоящее время доменное имя часто выступает объектом купли-продажи, а его оценочная стоимость временами существенно вырастает и может достигать нескольких миллионов долларов. Сам кибersквоттинг не является криминальным явлением. Таковым он становится, когда на его основе злоумышленники занимаются вымогательством, мошенничеством и другими видами преступной деятельности.

• другое (мошенничество в онлайн играх, мошенничество при онлайн платежах, мошенничество с трафиком и так далее).

Глава 2. Криминалистическая характеристика технологий совершения компьютерных преступлений.

2.1 Средства совершения компьютерных преступлений, их классификация

Компьютерное преступление является видом уголовного правонарушения, которое выделяется на основе обязательного присутствия в его составе признака объективной стороны: средства совершения киберпреступления.

Исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить взаимосвязь между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

Киберпреступления всегда совершаются с помощью средств компьютерной техники. Это комплексное понятие, включающее в себя компьютеры (стационарные ПК, планшеты, смартфоны и т.д), проводные и беспроводные компьютерные технологии (Wi-Fi, LTE и др.), а также программное обеспечение, находящееся в открытом обороте, запрещенные или ограниченного назначения, бесплатно распространяемые программы, а также модифицированное программное обеспечение.

Телекоммуникационная сеть имеет непосредственную связь со способом совершения киберпреступления в тех случаях, когда она подключена к программно-техническим устройствам или через нее распространяется вредоносная программа, которые являются средством или орудием совершения таких преступлений.

В этом плане вредоносные компьютерные программы и программно-технические средства могут являться как орудием, так и средством совершения преступлений, составляющих киберпреступность. Сущность средств и орудий совершения преступлений как признаков объективной стороны не зависит от характера преступных деяний, а определяется их ролью в совершенных преступлениях. При помощи средств и орудий совершения преступления оказывается преступное воздействие на общественные отношения, охраняемые уголовным законом.

Главным отличием орудия от средства совершения преступления является то, что они соотносятся друг с другом как род и вид. Если вредоносная программа или программно-техническое средство используются для облегчения совершения преступления, то они должны рассматриваться в качестве средства совершения преступления, а если при помощи вредоносной программы или программного средства непосредственно совершается преступление, то они могут рассматриваться в качестве орудия преступления.

Так, в преступлениях, связанных с шифрованием пользовательской информации, с последующим требованием выкупа за разблокировку, вредоносная программа используется в роли орудия совершения преступлений, а если данная программа использовалась, например, для похищения определенных сведений с целью дальнейшего шантажа (ст. 163 УК РФ), то она может рассматриваться в качестве средства совершения преступления.

В последнее время очень распространены случаи взлома чужих электронных ящиков. Владельцев шантажируют публикацией содержимого электронного ящика, предлагая им выкупить пароли от своей же почты у хакера, которые тот взломал и сменил.

Таким же способом похищаются сведения, которые являются объектами интеллектуальной собственности, а также данные, которые составляют коммерческую тайну и так далее.

Средства, которые используются при совершении преступлений в сфере компьютерной информации, достаточно разнообразны. Важно также, что с криминалистических позиций некоторые авторы классифицируют их по существенно различным критериям: по законности происхождения; по источнику происхождения; по техническому содержанию; по технологии использования и др.

Далее мы рассмотрим некоторые основания для классификации.

Средства, которые предназначены для полного или частичного управления компьютером и доступа к информации, которая на нем хранится, разграничивается на две группы - законные и незаконные.

Законные средства - могут быть разрешенными для общего использования и свободно распространяемыми, а также находиться в ограниченном обороте или быть изъятыми из оборота.

Ограниченные в гражданско-правовом обороте средства, например, предназначенные для негласно получения информации путем видеоаудиозаписи, могут быть приобретены при наличии соответствующего разрешения.

Использование изъятых из оборота специальных средств может быть разрешено правоохранительным или государственным органам (следственный комитет, прокуратура, суд, экспертные учреждения), однако создавать, владеть, пользоваться и распоряжаться такими средствами гражданам запрещено законом,

то есть их использование гражданами является незаконным.

По источнику происхождения средства совершения компьютерных преступлений их можно разделить на готовые, модифицированные, и средства собственной разработки[7].

Киберпреступниками могут использоваться готовое программное обеспечение либо модифицированное, а также средства собственной разработки. Это наиболее характерно для высокотехнологичных способов совершения компьютерных преступлений, при которых используются компьютерные программы, созданные членами преступной группы или посторонними специалистами по заказу преступников.

По технологии использования средства совершения компьютерных преступлений можно разделить на средства с удаленным доступом и без удаленного доступа.

В настоящее время в большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение. Это принципиальное обстоятельство имеет следствия, исключительно важные как для расследования, так и для предотвращения компьютерных преступлений.

Использование вредоносного программного обеспечения при удаленном доступе по информационным сетям позволяет осуществить преступление одновременно в отношении целых компьютерных систем. При таком доступе преступникам не нужно проникать в помещение, в котором находится объект посягательства, злоумышленники при этом не оставляют так называемых «цифровых следов». «Цифровой след» всегда возникает в результате работы и воздействия компьютерных программ.

Специфичность этих следов, проявляющаяся в отсутствии традиционных криминалистических характеристик, таких как форма, запах, цвет, и других, в которых могли бы отразиться, например, ДНК киберпреступника, папиллярный узор и т.д., создают существенные затруднения при расследовании компьютерных преступлений.

По техническому содержанию рассматриваемые средства можно с определенной долей условности разделить на аппаратные, программные и программно-аппаратные.

При незаконном доступе к объекту посягательства использование только аппаратных средств мало распространено, так как современные компьютерные устройства обычно обладают каким-либо собственным программным обеспечением.

Таким образом, в теории отсутствует единый подход к криминалистической классификации средств совершения киберпреступлений. Эта проблема всегда будет существовать в рассматриваемой системе, так как злоумышленниками создаются новые средства для совершения преступлений, а также совершенствуются уже имеющиеся. На данном этапе, учитывая все особенности киберпреступлений, для их эффективного расследования целесообразно провести классификацию средств совершения компьютерных преступлений, по критерию, которым, по моему мнению, является их техническое содержание.

Изучив статистические исследования о расследованиях компьютерных преступлений в России, можно сделать вывод, что наиболее часто используемыми средствами совершения киберпреступлений являются программные и аппаратно-программные средства.

Следует отметить, что выбор средства совершения преступления киберпреступником напрямую связан с его целью и мотивом, которые являются психологической основой поведения любого человека.

Далее нами проведен анализ основных средств совершения киберпреступлений, а также дана характеристика киберпреступников и выделены их наиболее распространенные типы.

В настоящее время, используемое киберпреступниками программное обеспечение очень разнообразно. Это разнообразие обусловлено тем, что, при написании программ, киберпреступникам необходимо учитывать особенности компьютерной системы, являющейся целью их атаки.

Рассмотрим самые распространенные, как показывает практика, программные средства из арсенала киберпреступников.

Существует множество вредоносных программ, их различных видов («вирусы» и «черви») и модификаций предназначенных для обхода систем защиты авторского права (взлом лицензий), для кибератак на системы безопасности, путем использования их уязвимостей и иные программы для совершения высокотехнологичных преступлений.

Сложность программного обеспечения, создаваемого киберпреступником, зависит от его уровня знаний и целей. Все эти элементы влияют на последствия киберпреступления. К примеру, мелкое мошенничество с использованием модификаций на основе общедоступного ПО, не сравнимо по последствиям с использованием ПО, предназначенного для несанкционированного доступа к данным, имеющим государственную тайну.

Высококвалифицированными программистами создается ПО, с помощью которого они способны получить доступ к счетам в крупнейших и наиболее защищенных от взлома (по заверениям служб безопасности) банках. Ущерб от таких «взломов», причиняемый банку, огромен. Однако следует отметить, информация о взломе компьютерной системы банка в подавляющем большинстве таких случаев сохраняется в тайне в целях сохранения репутации финансового учреждения. Думаю, это относимо не только к банкам, но и иным организациям.

Вредоносная программа может распространяться как злоумышленниками напрямую (например, загрузка в систему инсайдером), так и побуждать пользователей загружать и (или) запускать ее на своих компьютерных системах (рассылка через электронную почту, предложение обновить приложение до более новой версии и т.п.).

Сложность вредоносного программного обеспечения оценивается по сложности достижения цели, поставленной перед ним и наличия средств маскировки данной программы. В последнее время развивается тенденция использования вредоносных программ как часть многоступенчатых атак. Чаще всего вредоносное ПО используется для:

• неправомерного доступа к информации, или скачивания и закачивания данных (например, сбор электронных адресов для дальнейших спам- рассылок);

• похищение данных, составляющих тайну или имеющих ценность (идентификационные данные, коды, пароли и т.п.);

• несанкционированного доступа к третьим ресурсам посредством внедрения в компьютерную систему;

• создания помех в работе компьютерной системы и так далее.

Самой известной вредоносной программой является троянская программа, также известная в среде программистов как «троян» и «троянский конь».

Рассмотрим на ее примере принцип действия большинства вредоносных программ. Как правило, они состоят из двух частей, - это Клиент, который используется стороной атаки и Сервер, запускаемый в системе жертвы. Такие программы могут находиться в компьютере ничего не подозревающего пользователя длительное время, проникая в сердце системы (реестр) или связываясь с обычными файлами или приложениями. Это приводит к тому, что, загружая операционную систему, открывая личный файл или запуская приложения, активируется и вредоносная программа.

Поскольку существуют различные формы и виды вредоносных программ, то разработка методов борьбы с ними является достаточно сложной задачей для специалистов в данной сфере. Всю ситуацию можно обрисовать следующим образом: как нам известно, вредоносное ПО постоянно совершенствуется, поэтому разрабатываются антивирусные программы, имеющие обновляемые базы, в которых содержатся активные файлы по обнаружению и удалению вредоносных программ - сигнатурные базы. Очень важно, чтобы сигнатурные базы были актуальны. Их регулярное обновление позволит повысить эффективность и точность антивирусной программы.

Существует мнение, что для продвижения своих антивирусных программ разработчики порой сами создают вредоносное ПО. Целью такой деятельности может выступать банальная коммерциализация. Прибыль от продажи комплексных систем безопасности для крупных компаний и частным лицам огромна. Однако эта точка зрения представляется мне неверной. Написание вредоносных программ для антивирусных компаний является большим риском. Это может подорвать их репутацию, к тому же такая деятельность противозаконна. Более того, злоумышленников, желающих создавать вредоносное ПО, более чем достаточно. Таким образом, можно отнести подобные высказывания к разряду мифов.

Программно-аппаратными средствами являются технические приспособления с предустановленными программами, которые имеют своей целью считывание, хранение и передачу получаемых данных злоумышленникам. Рассмотрим наиболее распространенные в последнее время такие виды программно-аппаратных средств как кейлогеры и скиммеры.

Кейлогер - это программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш, дата и время нажатия, движения мыши.

Выделяются следующие типы кейлогеров:

• программные кейлогеры являются видом программного обеспечения, позволяющего осуществлять контроль над компьютерной системой. В настоящее время программные кейлогеры выполняют множество различных функций, например, перехват откликов мыши, фотографирование, перехват изображений с веб-камер и звука с микрофона, а также учет всех полученных и отправленных электронных писем.

• аппаратные кейлогеры - это миниатюрные устройства, фиксирующие последовательность нажатия клавиш на клавиатуре. Выполняются в различных формах и видах, могут крепиться к панели ввода данных или встраиваться в нее.

• акустические кейлогеры - являются аппаратными устройствами, позволяющими записывать и преобразовывать звуки, создаваемые пользователем в процессе нажатия клавиш.

Наиболее распространенны методами защиты от кейлогеров является использование антивирусных программ с актуальными сигнатурными базами.

Скиммер - небольшое портативное считывающее устройство, которое крепится к банкомату.

Скиммеры используют для кражи реквизитов банковских карт и данных владельца карты. Как правило, скиммер состоит из двух частей - устройства для считывания данных хранящейся на магнитной полосе банковской карты и устройства, позволяющего запечатлеть пин-код либо сохранить его.

Устройство для считывания данных с банковской карты крепится непосредственно к кардридеру, то есть к той части банкомата, куда вставляется пластиковая карта. Чаще всего считывающее устройство является пластиковой накладкой (см. рис.1).

Устройством для запечатления пин-кода обычно выступает миниатюрная камера, которая крепится рядом с панелью ввода пин-кода либо над ней. Иногда частью скиммера в виде специальной накладки может выступать кейлогер, который, как нам известно, сохраняет комбинацию цифр, вводимых владельцем банковской карты (см. рис.3).

Кейлогеры и скиммеры выполняются в самых различных модификациях. Некоторые из них позволяют злоумышленникам получать информацию в реальном времени с помощью беспроводной связи.

Число преступлений, совершаемых с использованием скиммеров и кейлоггеров неуклонно растет. Специалисты рекомендуют пользоваться банкоматами, которые расположены в отделениях банков либо на охраняемых территориях.

Посторонние элементы маскируют под цвет и форму банкомата, поэтому обнаружить скиммер на банкомате достаточно сложно. Производители банкоматов устанавливают них специальные устройства, распознающие скиммеры. Также банкоматы оснащаются специальными наклейками-инструкциями, в которых содержится описание банкомата. Если банкомат не соответствует указанному описанию, его использование не рекомендуется.

Таким образом, злоумышленники получают данные банковской карты и пин-код. В основном украденная информация используется для создания поддельных банковских карт и совершения онлайн покупок.

Стоит отметить, что существуют скиммеры, позволяющие снять копию данных с карты в тот момент, когда она оказалась в руках злоумышленника. Например, при расчете клиентов официанты, администраторы гостиниц или кассиры могут беспрепятственно скопировать данные банковской карты жертвы, а также завладеть пин-кодом.

Важно знать, что злоумышленники могут получить данные только с магнитной полосы вашей карты, но не со встроенного микрочипа. Поэтому карты с чипом являются наиболее защищенными.

Таким образом, владельцам банковских карт следует придерживаться следующих правил:

• не использовать банкоматы с подозрительными элементами конструкции;

• не передавать свою банковскую карту в чужие руки либо держать ее в поле зрения и следить за тем, чтобы она использовалась только по назначению;

• при вводе пин-кода стараться скрыть вводимые знаки от посторонних, а также камер наблюдения;

• использовать банковские карты с чипом.

2.2. Особенности личности киберпреступника

Знание основ психологии киберпреступника позволит объяснить выбор им средства совершения компьютерного преступления, а также поможет при разработке средств противодействия им, поскольку злоумышленники достаточно часто используют психологические приемы в своей деятельности.

Г.Т. Мегрелишвили делит киберпреступников на несколько групп[8]:

1. К первой группе автор относит лиц, отличительной особенностью которых является сочетание профессионализма и фанатизма в области компьютерной техники и программирования. Такие лица не имеют четкого противоправного намерения, действуют исключительно для проявления своих профессиональных и интеллектуальных способностей. Они любознательны и азартны. Повышение мер по обеспечению компьютерной безопасности рассматривают как вызов их способностям.

Особенности совершения киберпреступления данной группой лиц выражаются в отсутствии подготовки и плана действий, оригинальности способа совершения, а также в том, что меры по сокрытию преступления не принимаются.

2. Во вторую группу входят лица, страдающие информационными заболеваниями или компьютерными фобиями - это новым видом психических расстройств, тем не менее, признанных Всемирной организацией здравоохранения.

Киберпреступления, совершаемые этими лицами, чаще всего связаны с уничтожением компьютерных данных.

3. Третью группу лиц - являются высококвалифицированными специалистами, чаще всего имеющими высшее техническое образование. Однако, в отличие от первой группы, это профессионалы с устойчивыми преступными навыками и ярко выраженными корыстными целями.

Совершают киберпреступления многократно и принимают меры по сокрытию своих действий.

В своей статье «Общая характеристика психологии киберпреступника» А.Н. Косенковым и Г.А. Черным в зависимости от мотивации выделены следующие типы киберпреступников.

Корыстный тип. Помимо характерных для обыкновенного корыстного типа преступников свойств, киберпреступники могут совершать преступления для получения специфических предметов, имеющих особую ценность в

киберпространстве, например, хищение игровых предметов, учетных записей игроков, игровой валюты и иных предметов, без цели их дальнейшей продажи.

Насильственный тип. Несмотря на отсутствие физического контакта, такие насильственные преступления, как доведение до самоубийства или угроза убийством, могут быть совершены при помощи электронных устройств и сетей.

Сексуальный тип. Наиболее распространенная деятельность - незаконное распространение порнографических материалов или предметов, понуждение к действиям сексуального характера, развратные действия.

Социально-дезорганизующий тип. Основная цель - нарушение законодательно закрепленных социальных норм, разрушительное влияние на общественные отношения.

Идеологически или политически мотивированный тип, совершающий преступления по политическим или идеологическим убеждениям.

Статусный тип. Преступники этого типа, совершая преступления, стремятся получить высокий неформальный социальный статус. В среде киберпреступников статусность может иметь важное значение как мотив.

Исследовательский тип. Основой мотиваций данного типа является изучение программных и аппаратных составляющих электронных устройств и их сетей, поиск уязвимостей, возможности их использования и устранения.

Согласно исследованию Орли Тургеман-Голдшмита, лектора израильского университета, свою деятельность и цели киберпреступники истолковывают по-разному. Все они характеризуют себя как положительные и экстраординарные личности, которые являются носителями социальных изменений и демонстрируют лучшее поведение. Главным выводом исследования является то, что вины за свои преступные действия киберпреступники не ощущают.

Н.Н Федотовым также описаны несколько типичных образов киберпреступников.

1. «Хакер» (условное наименование). Основными мотивами данного типа являются исследовательский интерес, честолюбие, желание показать свои возможности. Наличие сложных средств защиты компьютерных систем и компьютерных данных воспринимаются хакерами как вызов своим способностям.

Казалось бы, что к подобному типу преступников должны относиться пользователи с высоким уровнем знаний в области IT. Однако практика показывает, что основная часть хакеров имеет средний уровень знаний. Можно предположить, что успехов в своей деятельности среднестатистический хакер достиг, получив конкретные знания в Сети - в настоящее время популярно выкладывать в Интернет различные инструкции (так называемые «гайды»).

2. «Инсайдер» (условное наименование). По мнению Н.Н. Федотова является наиболее распространенным типом киберпреступника, с невысоком уровнем знаний в области IT. Его отличительная особенность заключается в том, что в силу служебного положения он обладает доступом в информационную систему.

По мнению многих исследователей, большая «взломов» производится сотрудниками, то есть изнутри.

3. «Белый воротничок» (условное наименование). Данный тип представляется как заядлый казнокрад, для которого компьютерные системы стали новым инструментом преступной деятельности. Наиболее распространенными преступлениями, совершаемыми данным типом киберпреступника являются хищение средств, взяточничество, коммерческий подкуп и продажа информации, которая может составлять коммерческую тайну и так далее.

Среди «белых воротничков» могут выделяться личности, злоупотребляющие своим служебным положением из-за обиды на начальство или компанию и т.п., а также расхитители с полным отсутствием моральным принципов, которые занимаются данной преступной деятельностью только потому, что у них имеется такая возможность. Также Н.Н. Федотов выделяет и тех, кто попал в тяжелое материальное положение («квазивынужденные расхитители»).

4. «Е-бизнесмен» (условное наименование). Как правило, не является квалифицированным специалистом в области IT и не имеет служебного положения, которым может злоупотребить. Решение о совершении правонарушения принимается исключительно ради выгоды.

Выгодность киберпреступления в большинстве случаев связана со сложностью организации или технического обеспечения. Эти элементы влияют на успешность компьютерного преступления. Поэтому чаще всего «е-бизнесмены» отличаются хорошими способностями к предпринимательству и организации.

Данный тип преступников обычно занимается кардингом и фишингом.

5. «Антисоциальный тип» (условное наименование). В данном случае мотивом киберпреступника является социопатия, то есть патологическая тяга к подобного рода деятельности. Такие личности действуют импульсивно, так как не способны к предварительному планированию.

Считаем верным утверждение, что причиной девиантного поведения компьютерных пользователей является влияние, которое оказывает на их сознание киберпространство. Данная теория была предложена профессором Джоном Сулером (США). Им было введено понятие «эффект онлайн дезингибиции». Сущность данного эффекта заключается в том, что в условиях анонимности в киберпространстве люди отделяют свои действия и свою реальную личность, полагая, что может не брать на себя ответственность за свои действия, совершенные в киберпространстве.

Применение юридической психологии при расследовании компьютерных преступлений необходимо в силу отсутствия достаточного количества материальных следов преступника, разнообразия возможных мотивов киберпреступников, невозможность установления определенного круга лиц, которые могли совершить преступление, а также потенциально большой вред, который может нанести киберпреступление.

ЗАКЛЮЧЕНИЕ

Подводя итог проведенного исследования, обозначим некоторые положения из целого ряда выводов, на которых обосновывается данная работа.

1) Изучая различные подходы к определению понятий «киберпреступность» и «компьютерные преступления», мы согласились с мнением большинства исследователей, это преступность, связанная как с использованием компьютеров или компьютерных данных, так и информационных технологий и глобальных сетей, а также специального программного обеспечения. Потому понятия «киберпреступность» и «компьютерные преступления» в данной работе отождествлены.

2) Рассмотренные классификации компьютерных преступлений, основаны на таких критериях, объект посягательства, способ совершения, субъект преступления и уровень квалификации киберпреступника.

3) Понятие средств совершения компьютерных преступлений является комплексным и включает в себя аппаратные средства (компьютеры, планшеты, смартфоны и т.п.), а также программное обеспечение - программы и их модификации.

4) С развитием научно-технического прогресса создаются новые и совершенствуются уже имеющиеся у преступников средства совершения киберпреступлений. Потому их невозможно классифицировать. В рамках данной работы была принята классификация рассматриваемых средств по их техническому содержанию.

5) В настоящее время наиболее распространенными компьютерными преступлениями являются компьютерное мошенничество, неправомерный доступ к данным, имеющим ценность с целью их похищения и неправомерного использования.

Мы живем в эпоху информационного общества, и наша жизнь тесно связана с различными технологиями и сетью Интернет. И практически каждый раз, взаимодействуя с компьютерными технологиями, мы подвергаем себя угрозе стать жертвой киберпреступников. Потому всестороннее изучение средств совершения компьютерных преступлений позволит разработать эффективные меры по предупреждению и расследованию киберпреступлений.

Борьба с киберпреступлениями, которые являются серьезной угрозой для личности и государства на фоне происходящих в мире изменений, как одна из задач правоохранительных органов, выдвигается на приоритетные позиции.

Однако уже само выявление киберпреступления на данный момент представляет проблему, потому прослеживается высокая латентность преступлений в сфере IT.

В нашей стране отсутствует единая программа борьбы с киберпреступлениями. Для большинства сотрудников органов предварительного расследования раскрытие и расследование киберпреступлений представляет сложность, которая связана с тем, что при сборе доказательств и доказывании в таких делах необходимо изучение «виртуального следа». При этом уровень специальной технической подготовки, которая нужна для расследования подобных дел в органах юстиции очень низкий. К тому же отсутствует обобщенный материал следственной практики, методический материал и рекомендации по расследованию данного вида преступлений.

Эффективная работа экспертных подразделений ОВД и следователей-криминалистов СК РФ возможна при условии разработки специальных тактик проведения следственных действий, систематизации методик расследования киберпреступлений, а также подготовки специализированного кадрового состава. Все это, в совокупности, будет способствовать раскрытию киберпреступлений, даст возможность получать доказательства для предъявления их в суде.

На основании вышеизложенного можно сделать вывод, что российским криминалистам еще предстоит детально изучить киберпространство, разработать эффективные тактические и методические подходы к выявлению и расследованию киберпреступлений, которые в условиях глобального масштабирования более чем актуальны.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные акты и международные документы:

1. Уголовный кодекс РФ [Электронный ресурс]: Федеральный закон от 13.06.1996 № 63-ФЗ принят ГД ФС РФ // КонсультантПлюс: справ. правовая система. - Версия Проф. - Электрон. Дан. - М., 2016. - Доступ из локальной сети Науч. б-ки Том. гос. ун-та.

2. Бангокская декларация «Партнерство во имя будущего» (принята в г. Бангкоке 21.10.2003) // Дипломатический вестник. - 2003. - № 11. - С. 67 - 70.

3. Окинавская хартия глобального информационного сообщества (принята на о. Окинава 22.07.2000) // Дипломатический вестник. - 2000. - № 8. - С. 51 - 56.

Научные статьи:

4. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования / А.Г. Волеводз // Правовые вопросы связи. - 2017. - № 2. - С. 17 - 25.

5. Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний // Российская юстиция. - 2018. - № 2. - С. 14 - 15.

6. Головин А. Ю. Базовые криминалистические классификации преступлений // Известия Тульского гос. ун-та / Экономические и юридические науки. - 2013. - № 2

7. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Проблемы борьбы с отдельными видами преступлений. Криминологический журнал ОГУЭП. - 2012. - 3 (21). С. 87 - 94.

8. Лунев В. В. Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями, его место в истории конгрессов // Государство и право. - 2016. - № 9. - С. 95 - 100

9. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких тенологий // Вестник Том. гос. ун-та. - 2017. - № 299. - С. 180 - 181.

10. Мещеряков В.А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста: научный журнал. - 2013. - № 5 (10). - С. 265 - 270.

11. Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Компьютерная преступность и кибертерроризм: сборник научных работ. Запорожье: Центр исследования компьютерной преступности, 2014. Вып. 1. - С. 77 - 110.

12. Писарев Е. В. Информационное взаимодействие следователя с экспертом // Вектор науки ТГУ. - 2014. - № 3 (29). - С. 211 - 214.

13. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады ТУСУРа. - 2014. - № 2 (32). - С. 162 - 166.

14. Попов И.А. Правовое и организационное обеспечение раскрытия и расследования преступлений в сфере компьютерной информации: состояние и пути совершенствования // Библиотека криминалиста. - 2013. - № 5 (10). - С. 314 - 327.

15. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. - 2017. - № 24. - С. 43 - 46.

16. Чекунов И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. - 2012. - С. 9 - 22.

17. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. - 2017. № 2. - С. 37 - 44.

18. Шевченко Е. С., Михайлюченко Н. Н. Киберпространство как элемент обстановки совершения преступлений // Академический юридический журнал. - 2015. - № 2. - С. 52 - 59.

Диссертации и авторефераты диссертаций:

19. Васильев А. А. Судебная аппаратно-компьютерная экспертиза. Правовые, организационные и методические аспекты: дис. ... канд. юрид. наук. - М., 2013. - 246 с.

20. Вехов В.Б. Криминалистическая характеристика компьютерных преступлений : автореф. дис. ... канд. юрид. наук / Б.В. Вехов. - Волгоград, 2015. 27 с.

21. Воробьев В. В. Преступления в сфере компьютерной информации: Юридическая характеристика составов и квалификация: дис. ... канд. юрид. наук. - Н.Новгород, 2000. - 201 с.

22. Давыдова Н. Н. Криминалистические классификации преступлений и методик их расследования (теоретические проблемы): автореф. ... канд. юрид. наук. - Саратов, 2019. - 26 с.

23. Егорышев А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации: дис. ... канд. юрид наук. - Уфа, 2014. - 230 с.

24. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет : автореф. дис. ... канд. юрид. наук. Саратов, 2017. С. 16.

25. Остроушко А. В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации: дис. . канд. юрид. наук. - Волгоград, 2000. - 226 с.

26. Полстовалов В. А. Процессуальные, нравственные и психологические проблемы криминалистической тактики на современном этапе: автореф. ... д-ра юрид. наук. - Уфа, 2019. - 56 с.

27. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологические характеристики : дис. ... канд. юрид. наук. - Иркутск, 2016. - 237 с.

28. Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук. - Красноярск, 2010. - 206 с.

29. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно - правовые меры борьбы : автореф. дис. ... канд. юрид. наук. Владивосток, 2015. - 25 с.

30. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : автореф. дисс. ... канд. юрид. наук. - Москва, 2016. - 29 с.

31. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : дисс. ... канд. юрид. наук. - Москва, 2016. - 249 с.

Учебная литература и монографии:

32. Батурин Ю.М. Проблемы компьютерного права / Ю.М. Батурин. - М. : Юрид. лит., 1991. - 272 с.

33. Васильев А.А. Электронные носители данных как источники получения криминалистически значимой информации: учебное пособие / А.А. Васильев, К.Е. Демин. - М.: МГОУ, 2019. - 200 с.

34. Ветров Н.И. Уголовное право: учебник. Общая часть / Н.И. Ветров, Ю.Г. Ляпунов. - М. : Новый юрист, 2017. - 767 с.

35. Волчинская Е.К. Защита персональных данных: Опыт правового регулирования / Е.К. Волчинская. - М.: Галерея, 2001. - 236 с.

36. Дремлюга Р.И. Интернет-преступность: монография. - Владивосток, Изд-во Дальневост-го ун-та. - 2018. - 240 с.

37. Дуленко В.А. Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: учебное пособие / В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков. - Уфа: УЮИ МВД России, 2017. - 187 с.

38. Завидов Б. Д. Обычное мошенничество и мошенничество в сфере высоких технологий: практическое пособие / Б. Д. Завидов - М. : Приор, 2012. - 32 с.

39. Здравомыслов Б.В. Уголовное право Российской Федерации: Общая часть / Б.В. Здравомыслов. - М. : Юристъ, 2012. - 480 с.

40. Кравец С.Л. Большая Российская энциклопедия: В 30 т. Т.14 / С.Л. Кравец. - М., 2019. - 750 с.

41. Кустов А.М. Криминалистика и механизм преступлений: цикл лекций / А.М. Кустов. - Воронеж, 2002. - 304 с.

42. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков. - Воронеж: Изд-во Воронеж. гос. ун-та, 2012. - С. 94 - 119

43. Поляков В. В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон по преступлениям в сфере компьютерной информации: Сб. м-лов криминалистических чтений / В. В. Поляков; А. В. Шебалин; под ред. Ю. Л. Бойко. - Барнаул, 2013.

44. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов - М.: Норма. 2017 - 210 с.

45. Степнов Е.А. Информационная безопасность и защита информации: учебное пособие / Е.А. Степнов, И.К. Корнеев. - М.: Инфра-М, 2017. - 304 с.

46. Тушканова О. В. Терминологический справочник судебной компьютерной экспертизы: справочн. пособие / О.В. Тушканова. - М. : Макс Пресс, 2015. - 260 с.

47. Федотов Н.Н. Форензика - компьютерная криминалистика / Н.Н. Федотов. - М. : Юрид. мир, 2017. - 432 с.

48. Шурухнов Н.Г. Расследование неправомерного доступа к компьютерной информации: учебное пособие / Н.Г. Шурухнов. - М. : Московский ун-т МВД России, 2014. - 352 с.

1. Федотов Н.Н. Форензика - компьютерная криминалистика / Н.Н. Федотов. - М. : Юрид. мир, 2017. - с.36 ↑

2. Суслопаров А. В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук. - Красноярск, 2010. - с.127 ↑

3. Рассолов И.М. Право и Интернет. Теоретические проблемы / И.М. Рассолов - М. : Норма. 2016 - с.98 ↑

4. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологические характеристики : дис. ... канд. юрид. наук. - Иркутск, 2016. - с.127 ↑

5. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. - 2018. № 2. - С. 37 ↑

6. Федотов Н.Н. Форензика - компьютерная криминалистика / Н.Н. Федотов. - М. : Юрид. мир, 2017. - с.127 ↑

7. Попов И.А. Правовое и организационное обеспечение раскрытия и расследования преступлений в сфере компьютерной информации: состояние и пути совершенствования // Библиотека криминалиста. - 2013. - № 5 (10). - С. 314 ↑

8. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких тенологий // Вестник Том. гос. ун-та. - 2017. - № 299. - С. 180 ↑