ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ОТДЕЛЬНЫЕ АСПЕКТЫ

Учебное пособие

Уфа 2023

УДК 343.985.7:[343.3/.7](470)(075.8)
ББК 67.523(2Рос)я73-1
П83

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:

кандидат юридических наук, доцент А. Ш. Габдрахманов
(Казанский юридический институт МВД России);
кандидат юридических наук, доцент Л. Д. Матросова
(Орловский юридический институт МВД России имени В. В. Лукьянова)

Коллектив авторов:

Гурьянова В. Р. (кандидат физико-математических наук, б/з);
Тугузбаев Г. А., (б/с, б/з);
Ишмеева А. С. (кандидат экономических наук, доцент);
Рахматуллин М. А. (кандидат экономических наук, доцент);
Диваева И. Р. (кандидат юридических наук, доцент);
Пейзак Р. И. (кандидат юридических наук, б/з);
Абдразяпов Р. Р. (кандидат юридических наук, б/з);
Нугаева Э. Д. (кандидат юридических наук, б/з);
Харисова З. И. (кандидат технических наук, б/з);
Низаева С. Р (кандидат юридических наук, б/з);
Лонщакова А. Р. (кандидат юридических наук, доцент)

П83 **Противодействие преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий: отдельные аспекты** : учебное пособие / В. Р. Гурьянова, Г. А. Тугузбаев, А. С. Ишмеева [и др.] . – Уфа : Уфимский ЮИ МВД России, 2023. – 48 с. – Текст : непосредственный.
ISBN 978-5-7247-1158-6

В учебном пособии отражены основные направления обеспечения информационной безопасности, а также отдельные вопросы деятельности подразделений органов внутренних дел Российской Федерации, направленные на борьбу с преступлениями, совершаемыми с использованием современных информационно-телекоммуникационных технологий.

Учебное пособие предназначено для обучающихся образовательных организаций МВД России.

УДК 343.985.7:[343.3/.7](470)(075.8)
ББК 67.523(2Рос)я73-1

ISBN 978-5-7247-1158-6

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Системы информационных технологий постоянно совершенствуются благодаря развитию новых технических средств, методов обработки, передачи и хранения данных, а также усовершенствованию форм взаимодействия между компонентами. Вместе с этим, преступления, совершаемые с использованием технологий связи, все еще остаются актуальной проблемой. Основными факторами, которые способствуют совершению таких преступлений, являются высокая степень анонимности преступников, возможность удаленного доступа к мобильным устройствам связи, компьютерам и сетевым аккаунтам потерпевших.

Ущерб, наносимый обществу от преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий, создает общественный резонанс, требует от органов внутренних дел адекватной реакции на состояние оперативной обстановки.

Целью учебного пособия «Противодействие преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий: отдельные аспекты» является изучение теоретических вопросов, позволяющих раскрыть отдельные аспекты противодействия преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий.

В учебном пособии авторы ставили перед собой задачу − раскрыть отдельные аспекты в противодействии преступлениям, совершаемым с использованием современных информационно-телекоммуникационных технологий, путем освещения следующих вопросов:

– рассмотрение основных видов средств программного обеспечения, наиболее часто используемых в киберпреступлениях;

– рассмотрение общих положений об использовании информационных-телекоммуникационных технологий в финансово-кредитной сфере;

– рассмотрение основных видов киберпреступлений;

– обобщение особенностей взаимодействия следователя с органами дознания при возбуждении уголовных дел и планировании расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (киберпреступления);

– рассмотрение особенностей формирования практических навыков противодействия IT-преступлениям;

– рассмотрение тактических особенностей производства отдельных следственных действий на первоначальном этапе расследования преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий;

– изучение отдельных особенностей выявления и раскрытия преступлений, совершаемых с использованием информационно-коммуникационных технологий.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Основы знаний об информационных технологиях, используемых в противоправных целях

Начало XXI века характеризуется отчетливо выраженными явлениями глобализации и перехода от индустриального общества к обществу информационному. Под воздействием научно-технического прогресса повсеместно внедряются новые информационные технологии, которые предоставляют уникальные возможности для быстрого и эффективного развития как государства в целом, так и отдельно взятой личности. Как следствие, информация превратилась в основной товар, обладающий значительной ценностью, в своеобразный стратегический ресурс.

Возникли понятия компьютерной преступности (киберпреступности), Интернет-преступности, информационной наркомании. Стремительно растет число преступлений в сфере интеллектуальной собственности и высоких (информационных) технологий. Перед правоохранительными органами РФ стала неотложная задача: на высоком профессиональном уровне раскрывать преступления в сфере высоких технологий.

Внедрение новых информационных технологий в деятельность правоохранительных органов осуществляется через построение локальных, региональных и общегосударственных отраслевых вычислительных сетей. Одним из основных компонентов информационных вычислительных сетей общего пользования является федеральный банк криминалистической информации. На практике такие банки данных реализованы в виде автоматизированных информационных систем (далее – АИС), массивы которых увязаны в единое информационное поле. Необходимо отметить, что центральную роль в раскрытии и расследовании преступлений играют централизованные и региональные оперативно-справочные, оперативно-розыскные и криминалистические учеты.

Информационные технологии представляют собой технологические процессы, охватывающие информационную деятельность сотрудников органов внутренних дел.

Как и все технологии, информационные технологии находятся в постоянном развитии и совершенствовании. Этому способствует появление новых технических средств, разработка новых концепций и методов организации данных, их передачи, хранения и обработки, форм взаимодействия пользователей с техническими и другими компонентами информационно-вычислительных систем.

Информация, используемая в органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживае-

мой территории, о самих органах и подразделениях, их силах и средствах. В дежурных частях, у оперативных работников, участковых инспекторов полиции, следователей, сотрудников экспертно-криминалистических подразделений, паспортно-визовых аппаратов, других подразделений на документах первичного учета, в учетных журналах и на других носителях накапливаются массивы данных оперативно-розыскного и оперативно-справочного назначения, в которых содержатся сведения:

– о правонарушителях и преступниках;

– о владельцах автомототранспортных средств;

– о владельцах огнестрельного оружия;

– о событиях и фактах криминального характера, правонарушениях;

– о похищенных и изъятых вещах, предметах антиквариата;

– другая информация, подлежащая хранению.

В информационном обеспечении органов внутренних дел центральное место занимают учеты, которые используются для регистрации первичной информации о преступлениях и лицах, их совершивших.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления.

В качестве классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники:

– изъятие средств компьютерной техники (далее – СКТ);

– перехват информации;

– несанкционированный доступ к СКТ;

– манипуляция данными и управляющими командами;

– комплексные методы.

Способы совершения компьютерных преступлений подразделяются на несколько групп.

К первой группе относятся традиционные способы совершения обычных видов («некомпьютерных») преступлений, в которых действия преступника направлен на изъятие чужого имущества. Характерной отличительной чертой данной группы способов совершения компьютерных преступлений будет тот факт, что в них средства компьютерной техники

будут всегда выступать только в качестве предмета преступного посягательства.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемых в оперативно-розыскной деятельности правоохранительных органов.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся по борьбе с экономическими преступлениями.

§ 2. Общие положения об использовании информационно-телекоммуникационных технологий в финансово-кредитной сфере

Развитие цифровой экономики неотделимо от развития целого ряда технологий программирования, таких как искусственный интеллект, технологии облачных вычислений и распределенных реестров (блокчейн). За истекшее десятилетие произошло существенное распространение облачных сервисов, высокоскоростного доступа в сеть Интернет и сервисов удаленного хранения данных, что сделало возможным осуществление экономических операций и обмен огромными массивами данных и информации между людьми, предприятиями и устройствами. При этом появление инновационных разработок высокотехнологичных компаний, таких как Google и Apple, параллельно с распространением программного обеспечения как в виде программ с открытым кодом, так и в виде сервисов привело к повсеместному использованию смартфонов, компьютеров и серверов населением и предприятиями. Эти платформы обусловили развитие инноваций и появление широкого спектра приложений во многих секторах экономики, что способно в конечном счете изменить облик всех отраслей народного хозяйства. Между тем платформы также создали в цифровой сфере новые возможности для предпринимательства, что не только позволяет создавать новые продукты, услуги и процессы, но и изменять прежние трудовые процессы и бизнес-модели, существовавшие до эпохи сети Интернета. Поэтому можно сказать, что цифровая экономика возникла в точке пересечения, где информационно-телекоммуникационные технологии

(далее – ИТТ) и пользователи этой технологии – как люди, так и предприятия – стали в социальном и экономическом плане все больше зависеть от цифровых способов передачи информации. Развитие цифровой экономики в отдельных странах определяется наличием цифровой инфраструктуры, которая в мире распределена неравномерно, и в этом плане развивающиеся страны по-прежнему отстают от развитых. Главная причина состоит в том, что во многих развивающихся странах «распространение облачных сервисов по-прежнему сдерживается высокими затратами, связанными с выделением дополнительной полосы пропускания международного трафика для получения доступа к расположенным за границей серверам и центрам сбора и обработки данных»[1]. Также растущие угрозы безопасности связаны с цифровизацией финансового сектора. Например, растущее распространение финансовых технологий, таких как цифровые валюты и криптовалюты, в значительной степени не регулируется, и отсутствует центральный надзорный орган, который бы регулировал виртуальные обменные курсы или осуществлял надзор. Виртуальные транзакции гораздо труднее отследить, а значит, они могут осложнить надзор и контроль над усилиями по борьбе с торговлей оружием, отмыванием денег или финансированием терроризма.

Растущая технологическая зависимость критически важных секторов также может создать новые точки уязвимости. Критическая зависимость от таких технологий, как постоянный доступ в сеть Интернет, снижает способность правительства предоставлять основные услуги в случае, если данные услуги окажутся под угрозой.

В зависимости от задач, которые решаются с помощью информационных систем, их можно разделить на следующие группы:

– системы учета (оперативного, статистического, бухгалтерского);

– системы анализа финансовой деятельности предприятия;

– системы анализа инвестиционных проектов и бизнес-планирования;

– системы моделирования и прогнозирования.

Системы учета предназначены для решения важных задач по сбору и организации информации. Это необходимо для последующего анализа и моделирования деятельности предприятия. К основным пакетам можно отнести «1 С: Предприятие», программные продукты фирмы «СКВ Контур», R/3 от компании SAP.

1С: Предприятие – программа для автоматизации учета деятельности предприятия. Предназначена в первую очередь для автоматизации бухгалтерского и налогового учета и подготовки регламентированной (обязательной) отчетности, а также для оперативного и управленческого учета.

---

[1] Ишмеева А. С. Развитие цифровой экономики в современных условиях // Форум. 2022. № 3(26). С. 184−187.

«Контур.Бухгалтерия» разработана для ведения бухгалтерии небольших компаний, расчета зарплаты и сдачи отчетности через сеть Интернет.

«Контур.Эльба» для самостоятельного ведения учета бизнеса, а также формирования и отправки отчетности в контролирующие органы.

В программе можно создавать различные документы (договоры, счета, акты, накладные, счета-фактуры и т. д.), формировать всю необходимую отчетность и сдавать ее через сеть Интернет.

Первичный анализ финансовой деятельности предприятия возможно провести средствами MS Excel, а для более детальной обработки данных существуют такие пакеты, как AuditExpert, программы «ИНЭК-АФСП», «Альт-Финансы», «Олимп: ФинЭксперт»

AuditExpert – программа, предназначенная для анализа, мониторинга и оценки финансового состояния предприятия. Находит широкое применение в финансовых отделах предприятий, в банковской и аудиторской сферах. AuditExpert присутствует на рынке в двух вариантах сборки – Standard и Professional.

Программа анализа финансового состояния предприятия включает:

1. Экспресс-анализ финансового состояния предприятия, который позволяет оперативно оценить финансовое состояние предприятия на основе бухгалтерского баланса предприятия и отчета о финансовых результатах.

2. Проведение анализа финансовых рисков. В ходе анализа используются следующие методики:

– анализ безубыточности позволяет оценить финансовую прочность фирмы;

– анализ ликвидности позволяет оценить платежеспособность предприятия;

– анализ структуры баланса позволяет оценить риск банкротства предприятия;

– анализ рентабельности собственного капитала предприятия.

3. Методику рейтинговой оценки финансового состояния заемщика, позволяющую оценивать целесообразность предоставления кредита или продления договора кредитования.

Преимущества системы:

1) наличие возможности автоматического создания экспертных заключений;

2) поддержка различных вариантов ввода данных: возможен ввод данных с клавиатуры или импорт из других программных продуктов;

3) возможность использования специальных настраиваемых шаблонов для создания отчетов по результатам проведенного анализа, с использованием таких элементов оформления, как графики, таблицы, диаграммы и пр.;

4) возможность с помощью встроенного в программу конструктора менять предлагаемые методы анализа либо применять методики собственной разработки;

5) способность автоматической обработки большого объема информации благодаря использованию базы данных;

6) возможность получения конечной документации в различных валютах при формировании отчетов.

Программный продукт «ИНЭК-АФСП» используется для проведения финансового анализа на предприятии.

Основные достоинства программы «ИНЭК-АФСП»:

1) при работе в программе возможно производить анализ с учетом особенностей отрасли и специфики хозяйственной деятельности фирмы;

2) возможно использование нетипичных методик финансового анализа;

3) в процессе анализа финансовой деятельности предприятий, входящих в состав холдинга, имеется возможность получить объединенные данные;

4) присутствует возможность сравнительного анализа деятельности предприятий и их ранжирования;

5) позволяет получать автоматическое заключение по финансовому состоянию предприятия.

«Альт-Финансы» – один из продуктов компании «Альт», которые представляют из себя автоматизированную модель на базе MS Excel. В качестве источника финансовой информации данная программа использует бухгалтерскую отчетность. Программа «Альт-Финансы» позволяет проводить основные виды анализа финансово-хозяйственной деятельности предприятия: анализ ликвидности, платежеспособности, рентабельности. Программа обеспечивает все необходимые отчеты и показатели для наиболее важных случаев анализа финансовой отчетности:

– ежегодных отчетов перед акционерами и инвесторами;

– оценка надежности контрагентов;

– оптимизация продуктового портфеля;

– ценообразования по новым направлениям и проектам.

«Олимп: ФинЭксперт» – профессиональная программа для анализа финансового состояния предприятия. Основной контингент, на который ориентирована программа – это руководство предприятий, ведущие финансисты, аудиторы, сотрудники банков. Благодаря тому, что программа содержит как отечественные, так и зарубежные методики анализа, продукт находит широкое применение в профессиональной среде, в качестве источника данных для финансового анализа использует внешнюю бухгалтерскую отчетность.

Благодаря применению в программе многофакторной модели «Дюпон» стали возможными расчеты основных финансово-экономических по-

казателей, а благодаря многофакторности модели возможно определение первопричин изменения показателей. Еще одной особенностью программы является заложенная разработчиками возможность прогнозирования финансовых показателей предприятия, например, баланса. Кроме того, есть функция моделирования последствий управленческих решений. В программе можно работать в различных режимах: проведение проверки отчетности, экспресс-анализ, полный анализ и др. Источниками данных для анализа в программе выступают: бухгалтерский баланс и приложения к нему.

Системы анализа инвестиционных проектов и бизнес-планирования. Данное программное обеспечение предназначено для проведения всесторонней оценки предполагаемых инвестиций в различные бизнес-проекты. Программные продукты производят расчеты всех основных показателей эффективности проектов.

С увеличением потоков данных и передачи информации возникают опасения по поводу целостности передаваемой информации, ее источника, характера и цели. Сообщения средств массовой информации о предполагаемых кампаниях, направленных на искажение доказательств или подрыв фактов, стали более распространенными и появляется все больше свидетельств целенаправленной дезинформации, осуществляемой ради экономической выгоды или для того, чтобы намеренно обмануть общественность и нанести вред обществу. Целенаправленная дезинформация и манипулирование информацией, например, путем взлома, могут оказывать прямое влияние на критически важные сектора и процессы, в частности, подрывая демократический выбор и социальную сплоченность, или искажая политические решения правительства (например, в отношении крупномасштабных государственных инвестиций, таких как инвестиции в критически важные инфраструктуры и сектора).

Целью дезинформации и искажения фактов является намеренное влияние на политику или мнения тех, кто подвергается ее воздействию. Мотивы использования дезинформации могут быть стратегическими или экономическими, например, те, кто ведет такую деятельность с целью получения доходов от рекламы или другой финансовой выгоды. В итоге, субъекты, участвующие в подрыве целостности информации, стремятся манипулировать информационной средой, которая лежит в основе процессов принятия решений на национальном уровне. Низкоуровневые, более изощренные атаки дезинформации могут использоваться для искажения общественного мнения. Восприятие событий или проблем, подрывает доверие общества к государственным институтам, усиливает социальные разногласия и страх. В итоге это может подорвать социальную сплоченность и устойчивость, угрожая внутренней стабильности и эффективному функционированию общества.

Отличительная черта цифровой экономики, на которую все чаще обращают внимание – это ее способность предлагать различные решения в виде «сервисов», обеспечиваемых широкой доступностью облачной инфраструктуры и облачных вычислительных технологий. Доступность облачных сервисов позволила цифровой экономике превратиться в гораздо более многообразную среду, причем сами эти сервисы играют важнейшую роль в формировании глобальной экономики.

Можно выделить несколько составляющих цифровой экономики:

– стоимость активов. Доступность инфраструктуры облачных сервисов позволяет фирмам сокращать затраты на лизинг или аренду аппаратных средств и скачивание программ и приложений, а также по требованию управлять доступом к приложениям или системе хранения данных через поставщика облачного сервиса.

Это повышает мобильность предприятий, позволяя им сосредоточить усилия на профильных услугах. Наличие на платформах прикладных программ и «приложений-сервисов» сокращает дублирование затрат и повышает производительность, так как эти программы можно использовать для выполнения аналогичных задач или адаптировать под выполнение новых, что означает, что программный код не надо писать заново. Это сокращает затраты времени и средств разработчиков и повышает производительность их труда. С течением времени и с ростом использования программного кода число приложений и инструментов, доступных пользователям, увеличивается. Кроме того, доступность приложений-сервисов создает среду, ускоряющую развитие и повышающую производительность;

– сетевой эффект. Успех платформы зависит от способности привлечь достаточное количество пользователей с обеих сторон рынка (клиентов и работников). Для этого используются стратегии как связанные, так и не связанные с ценообразованием – например, бесплатный доступ или выгодные предложения. Эти стратегии повышают ценность платформы для пользователей, привлекая еще большее их число для создания критической массы – сетевого эффекта. Кроме того, в целях инноваций и повышения своей ценности платформы привлекают и стремятся удержать сторонних разработчиков за счет полностью или практически бесплатного доступа к приложениям и инструментам. Все это служит для создания сетевого эффекта;

– датафикация. Рост вычислительных мощностей и доступность облачных сервисов хранения данных позволили обеспечить сбор, хранение и анализ огромных массивов данных с гораздо большей скоростью, чем когда-либо прежде. Данные стали составной частью работы платформ, поскольку их можно монетизировать, например, с помощью адресной рекламы, а также использовать для массы различных целей, таких как прогнозирование поведения потребителей, улучшение продуктов (услуг) и управление работниками с помощью алгоритмов;

– мобильность. Инфраструктура облачных сервисов позволяет платформам работать в региональном или глобальном масштабе практически из любого места, вне зависимости от того, где находятся клиенты, поставщики или потребители. Отличительной чертой платформ является их способность с максимальной отдачей использовать нематериальные активы – программы, приложения и инструменты – которые являются основой их бизнеса.

§ 3. Преступления, совершаемые с использованием информационно-телекоммуникационных технологий (киберпреступления)

Европейская Конвенции о компьютерных преступлениях (Будапештская конвенция против киберпреступности)[1] в 2001 году была одним из первых нормативных правовых актов, обратившим внимание государств на необходимость применения законодательных и иных мер для квалификации в качестве уголовных преступлений умышленных лишения другого лица его собственности путем ввода, изменения, блокировки компьютерных данных, равно как и другого вмешательства в работу компьютерной системы[2]. Справедливости ради стоит отметить, что еще в начале 90-х годов XX в. в Российской Федерации были приняты первые нормативные акты, которые можно отнести к сфере компьютерных технологий, однако посвящены они были другим вопросам.

На сегодняшний день в самом широком понимании к понятию киберпреступности относится любая преступная активность в виртуальном пространстве (киберпространстве). К киберпреступлениям можно уверенно отнести:

– мошенничество с электронной почтой и интернет-мошенничество;

– мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);

– кража финансовых данных или данных банковских карт;

– кража и продажа корпоративных данных;

– кибершантаж;

– атаки программ-вымогателей;

– криптоджекинг;

---

[1] Конвенция о компьютерных преступлениях (Будапешт, 23.11.2001). Доступ из справочно-правовой системы Консультант Плюс.

[2] Смирнова И. Г. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ : монография / Смирнова И. Г. и др. М. : Издательство Юрлитинформ, 2016. С. 17.

– кибершпионаж[1].

Как мы видим, в некоторых киберпреступлениях осуществляются прямые атаки на компьютеры или другие устройства с целью вывода их из строя[2]. В других киберпреступлениях компьютеры используются киберпреступниками для распространения вредоносных программных кодов, получения незаконной информации, хищения личных данных с целью совершения корыстных преступлений[3], то есть, в них компьютеры используются для совершения других преступлений[4].

Таким образом, использование сети Интернет или иной компьютерной сети, является неотъемлемым компонентом преступлений, совершаемых в киберпространстве.

Все вышеуказанные типы киберпреступлений условно можно разделить на две группы, взяв в качестве основания наличие или отсутствие элемента насилия:

Можно выделить категории киберпреступлений:

– ненасильственные преступления;

– насильственные, или иные потенциально опасные преступления.

В первую группу ненасильственных преступлений включаются противоправное нарушение владения в киберпространстве, различные виды киберхищений, кибермошенничество, реклама оказания незаконных услуг в сети Интернет[5] и другие киберпреступления.

Вторая группа таит в себе угрозу физической расправы, связана киберпреследованиями, детской порнографией, а также нередко с наиболее опасными проявлениями киберпреступности – киберэкстремизмом и кибертерроризмом.

Несмотря на то, что Россия приостановила свое участие, признав утратившим силу распоряжение Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о преступности в

---

[1] Тисен П. А. Противодействие вовлечению подростков в радикальные организации в Интернете // II Всероссийская научно-практическая конференция «Новые, появляющиеся и видоизменяющиеся формы преступности: научные основы противодействия (Долговские чтения)». Ростов н/Д, 2022. № 2. С. 57–60. // Российская криминалистическая ассоциация им. А.И. Долговой [сайт]. URL: http://crimas.ru/wp-content/uploads/2021/07/Maket-sbornika-materialov-Dolgovskie-chteniya-29.03.2021.pdf. (дата обращения: 26.03.2023)

[2] Гридина Ю. А. Киберпреступность как новая криминальная угроза / Ю. А. Гридина, А. А. Русскова // Интеллектуальные ресурсы – региональному развитию. Ростов н/Д, 2019. Т. 5. № 2. С. 299–304.

[3] Понятие киберпреступлений и методы защиты // Гражданская инициатива интернет политики [сайт]. URL: https://internetpolicy.kg/ (дата обращения: 26.03.2023)

[4] Советы по защите от киберпреступников // Лаборатории Касперского [сайт]. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 26.03.2023)

[5] Там же.

сфере компьютерной информации»[1], ее содержание для нас имеет значительный интерес. Любопытно, что вышеуказанный документ все виды киберпреступлений объединяет в пять групп.

Первая группа включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

Вторую группу составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами).

Правонарушения третьей группы связаны с содержанием данных или контентом[2].

Нарушение авторских и смежных прав относится к четвертой группе.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в пятую группу киберпреступлений.

На самом деле, разделить киберпреступления на отдельные категории не так просто, поскольку существует множество вариаций их совершения и с каждым днем они видоизменяются, а некоторые отличаются применением сложнейших наборов средств и техник, используемых для их совершения.

Вместе с тем, существует четыре наиболее распространенных способа, которыми пользуются киберпреступники:

– использование вредоносных программ, которое базируется на злоупотреблении компьютерами и сетями;

– DDOS атаки: создание огромного количества запросов к серверу или службе с использованием коммуникационных сетевых протоколов с целью вывода из строя объекта воздействия;

– комбинация «социальной инженерии» и вредоносного кода: жертву вводят в заблуждение или принуждают к определенным действиям (нажатию на ссылку в электронном письме, посещению сайта и т. д.), что впоследствии приводит к заражению системы при помощи первого метода, либо хищению имущества[3];

– незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д. В этом случае злоумышленники скрыва-

---

[1] О подписании Конвенции о киберпреступности : распоряжение Президента Российской Федерации от 15 ноября 2005 г. № 557-рп // Собрание законодательства Российской Федерации. 2005. № 47. Ст. 4929.

[2] Спиридонова Н. Е. Подходы к описанию динамики компьютерных преступлений // Информатика: проблемы, методология, технологии : сборник материалов XIX международной научно-методической конференции / под ред. Д. Н. Борисова. Воронеж, 2019. С. 1242−1246.

[3] Гукасян А. А. Методы киберкриминала // Аллея науки. Томск, 2018. Т.2. № 1 (17). С. 262−265.

ют свои следы посредством анонимных профайлов, шифрованных сообщений и других подобных технологий[1].

Нормативные акты большинства стран мира предусматривают уголовную ответственность за киберпреступления, при этом наказание варьируется от штрафа до смертной казни[2].

В России большинство киберпреступлений совершается в двух основных направлениях, что наносит колоссальный урон, как непосредственно российским гражданам и компаниям, так и Российской Федерации в целом.

Первое направление можно охарактеризовать как киберпреступления, совершаемые с использованием сети Интернет с целью получения коммерческой выгоды. Преступники для достижения вышеуказанной цели используют следующие типы атак как фишинг, кибервымогательство, финансовое мошенничество, использование IP-телефонии и методов социальной инженерии[3].

Преступники активно используют мобильную связь и IP-телефонию для совершения звонков потенциальным жертвам, посредством которых получают конфиденциальную информацию для несанкционированного доступа к системе дистанционного банковского обслуживания. На сегодняшний день данный метод называется «социальная инженерия».

В ходе телефонного разговора злоумышленник представляется сотрудником банковского учреждения и сообщает потенциальной жертве о подозрительной операции по карте со стороны третьих лиц, после чего просит сообщить номер банковской карты и верификационный код, а завладев персональными данными, получает доступ к лицевому счету.

В завершении хотелось бы остановиться на новом предмете преступлений для российского уголовного права, которое все чаще подвергается преступным нападениям. Речь конечно же идет о криптовалюте.

Несмотря на актуальность цифровых валют, правовое регулирование виртуальных активов в РФ появилось только несколько лет назад с принятием Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[4] (далее – Закон о ЦФА), вступившего в силу только 1 января 2021 года[5].

---

[1] Понятие киберпреступлений и методы защиты // Гражданская инициатива интернет политики [сайт]. URL: https://internetpolicy.kg/ (дата обращения: 26.03.2023).

[2] Там же.

[3] Гукасян А. А. Указ. соч. С. 262–265.

[4] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[5] Земельное законодательство: сборник документов / С. А. Боголюбов, О. А. Золотова. М. : Проспект, 2016.

Понятие «цифровая валюта» раскрывается в п. 1 ст. 3 Закона о ЦФА как совокупность электронных данных, которые содержатся в информационной системе. В ст. ст. 17, 19, 21, 22 Закона о ЦФА указывается, что цифровая валюта признается имуществом. К сожалению, данное понятие закреплено не для всего перечня правонарушений, и новый Закон о ЦФА позволяет признавать цифровую валюту имуществом лишь в отдельных случаях. Теория уголовного права предполагает, что предметом хищения может быть только вещь. Таким образом, уголовно-правовая оценка криптовалют не как предмета хищения влечет за собой негативное последствие в виде неполной охраны общественных отношений в сфере оборота криптовалюты и других виртуальных активов, поскольку квалификация преступлений, не связанных с хищением, предполагает указание способов совершения преступлений или предмета преступления. Для выработки единого подхода необходим отказ от физического признака предмета хищения, что соответственно приведет к изменениям в системе привлечения лиц к уголовной ответственности за преступления, имущественного характера. Анализ судебной практики показал, что криптовалюта может являться предметом взятки, однако вымогательство криптовалюты было исключено из общего объема обвинения, в связи с отсутствием правового статуса.

Криптовалюты и другие финансовые активы используются при совершении преступлений. Они выступают предметами взятки и коммерческого подкупа, платежным средством при осуществлении незаконной деятельности, связанной с отмыванием (легализацией денежных средств), незаконного оборота оружия и наркотиков, порнографических материалов и финансирования террористической деятельности и т. д.

ГЛАВА 2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Взаимодействие следователя с органами дознания при возбуждении уголовных дел и планировании расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (киберпреступления)

Рассматриваемые преступления все чаще совершаются технически оснащенными преступными группами (в том числе международными), характеризуются усложненными способами их подготовки и сокрытия, созданием и использованием вредоносных компьютерных программ.

Специфика стадии возбуждения уголовного дела обусловлена особенностью конкретного вида преступления, что определяет последовательность действий следователя (дознавателя) при обнаружении признаков такого преступления. Выявленные признаки оказывают влияние на выбор сил и средств, а также ход всего дальнейшего расследования.

В соответствии с требованиями закона решение о возбуждении уголовного дела любой категории возможно лишь при наличии соответствующего повода и оснований.

Во многом для решения вопроса о возбуждении уголовного дела будет способствовать правильная организация проведения доследственной проверки. Организация проведения доследственной проверки в каждой конкретной следственной ситуации будет иметь свою специфику, однако можно предложить некоторые рекомендации.

1. Подробно опросить заявителя об обстоятельствах совершенного преступления. Например, у заявителя возможно выяснить:

– дату, время поступления, кто имел возможность доступа к управлению счетами потерпевшего, в том числе к его мобильному телефону;

– поступали ли ему в период, предшествующий хищению денежных средств, СМС-сообщения или электронные письма с указанием попыток осуществления транзакций, которые он не совершал;

– абонентский номер телефона, банковской карты, банковского счета, на которые переведены денежные средства;

– имеются ли у него документы, подтверждающие факт списания денежных средств, а также общения с неустановленным лицом, совершившим хищение денежных средств (в том числе скриншоты, переписка);

– не было ли сбоев в работе аккаунтов в социальных сетях и т. д.

2. При наличии у потерпевшего документов, подтверждающих факт совершения хищения, изъять в установленном порядке.

3. Разъяснить заявителю/потерпевшему необходимость представления выписок из банков, сведений о входящих и исходящих соединениях операторов мобильной связи.

4. Для получения информации, содержащей банковскую либо иную охраняемую законом тайну, необходимо сформировать и направить запрос о предоставлении паспортных данных о владельце банковского счета, банковской карты или электронного кошелька, информации о движении денежных средств по счету, местах их обналичивания, о расположении банкоматов, камер видеонаблюдения, о привязанных абонентских номерах, об адресе офиса банка, в котором открыт счет, работе онлайн-банкинга, об IP-адресе устройства, с использованием которого оно осуществлялось через систему дистанционного банковского обслуживания.

В соответствии с требованиями ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» данная информация предоставляется: 1) на основании судебного решения должностным лицам органов, уполномоченных осуществлять оперативно-розыскную деятельность, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном ст. 9 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; 2) либо по возбужденному уголовному делу на основании запроса следователя, согласованного с руководителем следственного органа.

Зная первые шесть цифр номера пластиковой карты можно самостоятельно определить банк получателя денежных средств, используя интернет-портал https://psm7.com/bin-card.

5. Запросить информацию у операторов мобильной связи о соединениях между абонентами и (или) абонентскими устройствами.

Данная информация предоставляется в порядке, предусмотренном ст.ст. 186.1 и 165 Уголовно-процессуального кодекса Российской Федерации[1] (далее – УПК РФ), на основании постановления суда о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Запрашиваемая информация должна содержать сведения о паспортных данных владельца абонентского номера, дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, сведения об IMEI-коде абонентского устройства, о сетевом трафике, IP-адресах, использованных для входа в личный кабинет мобильного оператора, о входящих и исходящих платежах по лицевому счету, сведения о номерах и

[1] Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18 декабря 2001 г. № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

месте расположения приемопередающих базовых станций, а также векторе (азимуте) направления сигнала. Последний, как правило, представлен в числовом выражении и означает угол, под которым находилось абонентское устройство по отношению к базовой станции в момент фиксации его активности в сети. Используя эти данные, можно создать графическую схему предполагаемого местонахождения подозреваемого лица. При необходимости, привлечь сотрудника технической службы оператора связи.

Также необходимо запросить сведения об адресе торговой точки, продавце sim-карты, копию регистрационной формы.

При получении информации об IMEI-коде абонентского устройства звонившего необходимо дополнительно запросить сведения о всех sim-картах, использовавшихся на данном телефоне.

Установить принадлежность абонентского номера звонившего оператору мобильной связи возможно при помощи сайта Россвязи (https://www.rossvyaz.ru/activity/num_resurs/registerNum/).

6. В учреждениях связи по судебному решению могут быть изъяты сведения, которые с учетом требований ст. 53 Федерального закона от 7 июля 2003 г. № 126-ФЗ (ред. от 7 июня 2017 г.) «О связи»[1] (далее −ФЗ «О связи») распространяют на себя положения об их тайне.

Действующая практика позволяет на основании запроса о предоставлении сведений получать без судебного разрешения следующую информацию:

– об абоненте с указанием его установочных данных;

– о номере и дате заключенного договора об оказании телеметрических услуг с приложением заверенной копии договора;

– протоколы работы в сети Интернет (log-файлы),

– об IP-адресах, с которых осуществлялось создание и администрирование аккаунта;

– об абонентах, которым в указанный момент времени выдавался установленный IP-адрес;

– о MAC-адресах компьютерной техники и сетевого оборудования, с использованием которых осуществлялся доступ к сети Интернет.

7. Сформировать и направить запросы в организации, интернет-провайдерам, которым принадлежат почтовые сервисы, социальные сети, интернет сервисы, о предоставлении сведений, не являющихся информацией ограниченного доступа.

В соответствии с положениями ч. 1 ст. 53 ФЗ «О связи» сведения, позволяющие идентифицировать абонента либо его оборудование, данные систем расчета за оказанные услуги связи подлежат защите в соответствии с законодательством Российской Федерации, то есть на основании запроса предоставлены быть не могут.

---

[1] О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ (ред. от 7 июня 2017 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, уместно запрашивать следующую информацию:

– дату, время заведения электронных почтовых ящиков и иных ресурсов;

– сведения, указанные при регистрации электронного ресурса (ФИО, адрес, пол, возраст, абонентский номер, электронная почта и иные);

– IP-адреса, используемые для создания и администрирования объявлений, сайтов, электронной почты, анализ cookie-файлов.

С целью установления организаций-арендодателей хостинга и организаций-регистраторов необходимо воспользоваться интернет ресурсом www.reg.ru. У данных организаций запросить информацию о паспортных данных, абонентских номерах, электронной почте, IP-адресах, использованных для регистрации пользователя/аренды хостинга, для входа в личный кабинет или панель управления для администрирования, об оплате услуг регистрации и аренды с указанием полных реквизитов плательщика, анализ cookie-файлов.

Чтобы определить какому провайдеру выдавался IP-адрес, необходимо проверить его по специальному сервису «Whois», расположенному по адресу http://www.whois-service.ru/lookup/.

8. При установлении факта наличия видеозаписи в местах расположения компьютерного оборудования, при помощи которого было совершено преступление (банкоматы, POS-терминалы, терминалы самообслуживания), либо места свободного доступа к открытой точке доступа сети Wi-Fi (помещения торговых центров, мест общепита, транспорт и пр.), необходимо ее изъять надлежащим образом[1].

В случае возбуждения уголовного дела все обнаруженные и изъятые предметы (документы) могут иметь доказательное значение, поскольку могут быть отнесены к такому виду доказательств, который определяется законом как «иные документы» (п. 6 ч. 2 ст. 74 УПК РФ).

Для эффективного разрешения возникающих на этапе возбуждения уголовного дела вопросов следователю необходимо использовать возможности оперативных подразделений.

Вместе с тем необходимо уделять особое внимание качеству представляемых в следственные подразделения материалов для решения вопроса о возбуждении уголовного дела.

Как правило, материалы передаются в органы предварительного следствия уже зарегист в книге регистрации сообщений для принятия решения в порядке ст. 145 УПК РФ, зачастую с истекшими сроками, установленными для их рассмотрения. В этих случаях, не имея возможности процессуальными мерами дополнить проверочные материалы и устранить

---

[1] Жердев П. А. Электронно-цифровые следы как элемент криминалистической характеристики преступлений в сфере компьютерной информации. // Вестник Дальневосточного юридического института МВД России. 2020. № 2 (51). С. 94–101.

имеющиеся в них недостатки, следователи вынуждены отказывать в возбуждении уголовного дела, что влечет затем отмену руководителем следственного подразделения как незаконных и необоснованных.

Вместе с тем, взаимодействие следственных аппаратов с органами дознания способствует не только решению как общих, так и частных задач, стоящих перед ними, но и, что немаловажно, сближению этих задач, интеграции накопленных знаний, объединенных общей целью – борьба с преступностью.

§ 2. О формировании практических навыков противодействия IT-преступлениям

В настоящее время наблюдается всеобщая трансформация мирового сообщества в цифровое пространство, где все больше преобладают информационно-телекоммуникационные технологии, развивающиеся настолько стремительно, что в ряде случаев правоохранительные органы сталкиваются с проблемами в раскрытия профессионально организованных киберпреступлений. Развитие электронных систем платежей, повсеместное использование криптовалют, массовое внедрение умных устройств в жизнь человека, использование беспилотных и интеллектуальных систем, ежедневная передача значительных массивов пользовательских данных в сети Интернет и блокчейн, а также переход в онлайн-режим работы многих сфер жизнедеятельности общества (в том числе в связи с пандемией) неизбежно привело к росту преступлений, совершаемых и использованием информационных технологий не только в Российской Федерации[1], но и во всем мире[2].

Соответственно возникает острая необходимость в подготовке квалифицированных кадров, специализирующихся на борьбе с киберпреступностью, в целях эффективной фиксации, изъятия и использования цифровых доказательств, в частности, с использованием информационных-телекоммуникационных технологий.

Так, в настоящее время в образовательных организациях имеется возможность проводить практико-ориентированные занятия, направленные на приобретение обучающимися навыков обнаружения и фиксации

---

[1] Ежемесячный сборник о состоянии преступности в России (2010–2020 гг.) // Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации [сайт]. – 2021. URL: http://crimestat.ru/analytics (дата обращения: 26.03.2023).

[2] Paoli S., Johnstone J., Coull N., Ferguson I., Sinclair G., Tomkins P., Brown M., Martin R. A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists // Policing: A Journal of Policy and Practice. V. 15 (2). 2021. P. 1440.

цифровых артефактов в технических средствах[1], а также изъятия криминалистически важной для расследования и раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, информации[2] на базе компьютерных классов с использованием свободно распространяемого программного обеспечения в области компьютерной криминалистики[3].

Грамотное использование информационных-телекоммуникационных технологий в раскрытии и расследовании киберпреступлений в первую очередь связано с приобретением навыков противодействия такого рода преступности и является следствием выработки практических навыков в ходе обучения по тематикам практических занятий и соответствующим фабулам по кейс-методу обучения[4]. В этом свете предлагается рассмотреть возможность выработки практических навыков поиска криминалистически значимой информации с использованием программного обеспечения. Алгоритм ведения занятий, с использованием такого рода программного обеспечения, может быть следующим:

1. Преподаватель обозначает важность рассмотрения изучаемой темы, приводит конкретные примеры и ситуации, когда необходимо выявление криминалистически значимой информации в цифровом виде (например, определение перечня подключаемых к исследуемому техническому средству внешних устройств за заданный промежуток времени в качестве доказательства несанкционированного завладения защищаемой информацией путем копирования на определенный flash-носитель и т. п. задачи). Таким образом, моделируется конкретная ситуация, которая требует фиксации и изъятия того или иного цифрового доказательства[5].

2. Выдается инструкция и алгоритм поиска интересующей информации, определяется путь к файлам и каталогам операционной системы исследуемого технического средства, путь доступа в редакторе реестра.

3. Обучающимся предлагается отработать задачу поиска цифрового артефакта на собственном ПК, подготовить отчет проводимого исследования.

---

[1] Лонщакова А. Р. Возможность выявления криминалистически значимой информации при анализе реагирования на киберинциденты // Евразийский юридический журнал. 2021. № 2 (153). С. 338–339.

[2] Лонщакова А. Р. Выявление криминалистически значимых маркеров при анализе уровней защиты информации. Отдельные особенности работы с группами риска // Проблемы развития современного общества. Сборник научных статей 7-й Всероссийской национальной научно-практической конференции. Курск, 2022. С. 344.

[3] Hamad B., Mishra A. Analysis of web browser for digital forensics investigation // International Journal of Computer Applications in Technology. V. 65 (2). 2021. P. 161.

[4] Нугаева Э. Д., Куценко С. М. Деловая игра – одна из форм эффективного метода обучения // Вестник Уфимского юридического института МВД России. 2010. № 3. С. 12.

[5] Casey E., Thomas R. Digital transformation risk management in forensic science laboratories // Forensic Science International. V. 1. 2020. P. 316.

4. Предлагается подготовить необходимый и достаточный пакет процессуальных документов (по осмотру предмета (техники), изъятию данных и пр.).

5. Производится выборочный разбор сформированных отчетов по исследованию технических средств и пакетов документов, выявляются ошибки и замечания.

С целю автоматизированного оформления процессуального документа по фабуле задания обучающимся можно предложить использовать программу ЭВМ «Алгоритмический комплекс процессуальных действий при дистанционном мошенничестве «АКПД ДИСТАНТ», авторского коллектива Уфимского УЮИ МВД России, которая представляет собой инструмент анализа преступлений, связанных с дистанционным мошенничеством, а также средство определения алгоритма действий следователя на первоначальном этапе расследования хищений с использованием мобильных средств связи. Обучающимся предоставляется инструкция по работе с программой, предлагается оформить необходимый комплект процессуальных документов в автоматизированном виде исходя из условий и обстоятельств совершения преступления.

В случае моделирования ситуации, связанной с дистанционным мошенничеством, в том числе связанного с электронными платежными системами, обучающимся предлагается получить информацию, содержащую банковскую или иную охраняемую тайну, при этом в программе представлены рекомендации по определению наименования банка, оператора или провайдера услуг связи путем использования международных онлайн-сервисов в свободном доступе.

После получения информации о поставщиках услуг обучающимся предлагается подготовить необходимые процессуальные документы, при необходимости экспортировать полученные данные по киберинциденту в файл.

Таким образом, рассматриваемое программное обеспечение может быть использовано в учебных и научно-исследовательских целях: в рамках подготовки процессуальных документов и определения сведений о поставщиках услуг, расследования киберинцидентов в рамках изучения учебных курсов, связанных с приобретением навыков противодействия IT-преступности (в том числе в дистанционном формате). Освоение программы может осуществляться также путем использования в качестве стендовой ЭВМ персонального компьютера, находящегося в личном распоряжении обучающегося без предварительной установки (в случае дистанционного формата обучения).

В целях отработки практических навыков поиска цифровых доказательств (артефактов, цифровых следов преступлений), сканирования носителей информации, а также образов накопителей, поиска системных фай-

лов, анализа реестра и сетевых подключений[1] и т. п. каждым обучающимся в отдельности целесообразно применение методики проведения занятий в компьютерном классе в концепции работы на криминалистическом полигоне. При этом предполагается демонстрация отработки навыков на стендовой ЭВМ с визуализацией на интерактивной доске. В данном случае отработка практических навыков обучающимися предполагает извлечение важных для следствия данных, таких как: список пользователей операционной системы, сведения о последнем входе, времени смены пароля и пр., параметры автозагрузки (USB, CD, DVD), имя компьютера, местоположение системного журнала, список USB-устройств, когда-либо подключённых к системе, список подключённых устройств, последние файлы, открытые с помощью разных офисных приложений и пр., сетевые карты, дата установки, версия операционной системы, сведения конфигурационных файлов, программы, которые запускаются при входе в систему, время последнего выключения компьютера, временная зона, профили беспроводных сетей и пр. Кроме того, для каждого обучающегося важна отработка навыков поиска по извлечённым данным со следующей функциональностью: поиск по слову или фразе, поиск по файлу ключевых слов, поиск по регулярному выражению, формирование отчёта из полученных данных.

Эффективной методикой проведения практических занятий является отработка навыков в концепции киберполигона с использованием программного обеспечения «Мобильный Криминалист», т. е. с возможностью эксплуатации отечественного программного обеспечения для проведения криминалистической экспертизы ЭВМ, мобильных устройств, облачных сервисов, дронов и иных технических средств. Указанное программное обеспечение позволяет извлекать, сохранять и анализировать информацию с перечисленных устройств, провести полное «цифровое» расследование в рамках одного продукта.

На полигоне с использованием ПО «Мобильный Криминалист» возможно реализовать приобретение навыков по извлечению физических образов и резервных копий с различных мобильных устройств, в том числе на различных операционных системах и чипсетах процессоров, проведение анализа данных на различных хранилищах данных (машинные носители, облачные хранилища и пр.), осуществление импорта образов технических средств, проведения статистического и файлового анализа данных на исследуемых устройствах, построение графов взаимодействий и пр., извлечение учетных данных для авторизации на веб-сервисах и в информацион-

[1] Аминев Ф. Г., Давлетшина Л. С., Нугаева Э. Д. Назначение и производство судебных экспертиз в расследовании преступлений. Уфа : УЮИ МВД России, 2007.

ных системах, анализ почтовых агентов, а также, распознавание хранимых на устройстве изображений.

Таким образом, использование информационно-телекоммуникационных технологий, в частности, рассмотренного выше программного обеспечения в рамках проведения занятий по дисциплинам, связанным с приобретением навыков противодействия IT-преступности, позволят смоделировать максимально приближенные к реальным киберинцидентам условия, что позволит сформировать наиболее эффективную систему обучения и, соответственно, профессиональной адаптации к цифровой трансформации общества.

§ 3. Тактические особенности производства отдельных следственных действий на первоначальном этапе расследования преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий

На первоначальном этапе расследования проводятся такие следственные действия, как осмотр места происшествия, обыск, выемка, допросы и др. Все следственные действия по делам о преступлениях в сфере информационно-телекоммуникационных технологий проводятся в строгом соответствии с требованиями действующего уголовно-процессуального законодательства.

Рассматривая подготовительный этап осмотра места происшествия, следует отметить, что еще до выезда целесообразно получить объяснение физического лица или руководителя организации, в котором отразить вопросы, касающиеся функционирования компьютерного оборудования (наличие единого сервера, локальной сети, блокирования программ в случаях попытки несанкционированного доступа, наличия охранной сигнализации в целом). Отметим, что дистанционное блокирование помещения зачастую связано с механизмом самоуничтожения криминалистически значимой информации на жестком диске, действие которого определяется вмонтированным в него источником питания. Физические и юридические лица, эксплуатирующие данные механизмы, часто имеют скрытую систему резервирования данных. Необходимо выяснить наличие паролей, электронных ключей, правил их использования для получения доступа к имеющей значение для расследования информации.

Целесообразно выявить наличие резервного копирования информации в конце рабочего дня с ведением протокола деятельности компьютерной техники за день, так как при отлаженном механизме резервирования это вполне может быть осуществимо. Перед производством рабочего этапа осмотра рекомендуется ознакомить специалиста, который будет участвовать в следственном действии, с материалами доследственной проверки.

Целью осмотра места происшествия является установление конкретного средства вычислительной техники и компьютерной информации, которая может выступать в качестве предмета либо орудия совершения преступления и нести в себе следы преступной деятельности[1].

В состав следственно-оперативной группы по указанной категории уголовных дел рекомендуется включить: специалиста-криминалиста, который будет работать по выявлению, фиксации и изъятию материальных следов преступления; специалиста в сфере компьютерной техники. При необходимости помощь при проведении данного следственного действия могут оказать специалисты в области бухгалтерского, банковского дела и т. д. Ответственность за полноту и качество осмотра места происшествия несет лицо, руководящее расследованием.

Рабочий этап характеризуется сбором криминалистически значимой и доказательственной информации. Необходимо сфотографировать место осмотра и незамедлительно предпринять действия по недопущению уничтожения или сокрытия компьютерной информации. Следует отстранить физическое лицо или работников организации от компьютерной техники, разместив их, по возможности, в отдельном помещении.

В начале осмотра с помощью специалиста устанавливается функциональное назначение компьютерной техники, находится ли она в рабочем состоянии, имеется ли в памяти информация. Кроме того, следует установить наличие или отсутствие сопряжения с каналом электросвязи и другими техническими устройствами. После этого необходимо перейти к поиску следов, содержащихся на корпусе, отдельных деталях и проводных соединениях, в постоянной и оперативной памяти[2]. При наличии локальной сети необходимо найти сервер, в котором размещена часть информации, и от которого зависит работа всех ее элементов. Для предотвращения модификации или уничтожения информации с удаленных рабочих мест, которые могут находиться на некотором расстоянии от осматриваемого объекта, рекомендуется определить наличие кабелей и проводов, ведущих в другие помещения от самой компьютерной техники. Вместе с тем, необходимо определить, поступает ли информация на компьютер путем факсимильной, электронной или телетайпной связи.

При осмотре монитора необходимо зафиксировать информацию на нем. В ходе детального осмотра выявить программы, запущенные на компьютере, подключения внешних кабелей, чтобы в последующем правильно

---

[1] Сысенко А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений // Закон и право. 2020. № 12. С. 216–218.

[2] Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. М. : Издательство Юрайт, 2022. С. 82 // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/496747 (дата обращения: 26.03.2023).

восстановить их соединения. Программы зашифровки и уничтожения информации, запущенные на осматриваемом компьютере необходимо приостановить и начать осмотр именно с него. Процесс введения текста на компьютере может заинтересовать следствие, в связи с этим рекомендуется его сохранить.

Следы могут быть выявлены при обнаружении специальных средств опознания пользователя персонального компьютера. К ним относятся:

– электронные карты, куда записывается информация о владельце, ведется учет всех операций, выполняемых им;

– электронные ключи доступа к персональному компьютеру и ключи электронно-цифровой подписи;

– устройства дактилоскопической идентификации пользователя по отпечаткам пальцев;

– устройства опознания пользователя по почерку, для чего используются динамические (скорость, давление на бумагу) и статические (форма и размер подписи) характеристики процесса подписи;

– устройства опознания пользователя по голосу, сетчатке глаза.

При наличии подобных устройств, подключенных к компьютеру, в них производится автоматическая фиксация незаконных попыток вторжения. Специализированные системы считывают информацию с магнитных карт несанкционированного доступа, записывают голос, фиксируют отпечатки пальцев. Эти данные могут быть использованы для идентификации личности преступника.

В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства компьютерной техники (например, если компьютер является сервером или рабочей станцией компьютерной сети), после осмотра необходимо блокировать соответствующее помещение, отключить источники энергопитания аппаратуры[1].

При изъятии информации из оперативной памяти компьютера (оперативного запоминающего устройства) следует копировать ее на физический носитель с использованием сертифицированного программного обеспечения.

С позиции криминалистики в рамках уголовного процесса в целях выявления и раскрытия преступлений также может быть предложена тактика осмотра сетевой активности[2], имеющей доказательственное значение. Интернет-сайт может рассматриваться как разновидность документа, особен-

---

[1] Низаева С. Р. Цифровые технологии в криминалистике // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2021. № 21 (1). С. 55–56.

[2] Архипова И. А. Актуальные проблемы расследования преступлений в сфере компьютерной информации : сборник статей международной научно-практической конференции // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения). М., 2018. С. 28–34.

ность которого заключается лишь в специфической форме представления компьютерной информации, не меняя самой сути понятия документа[1].

В протоколе осмотра компьютера фиксируют:

– его тип (назначение), марку (название), конфигурацию, цвет и заводской номер (серийный, инвентарный или учетный номер изделия);

– тип (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов; состояние на момент осмотра (выключено или включено);

– техническое состояние – внешний вид, целостность корпуса, комплектность (наличие и работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой), наличие расходных материалов, тип используемого машинного носителя информации;

– тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенного к нему электрооборудования, количество питающих электроразъемов-розеток и т. д.);

– наличие заземления («зануления») и его техническое состояние;

– наличие и техническая возможность подключения периферийного оборудования и(или) самого компьютера к такому оборудованию либо к каналу электросвязи;

– имеющиеся повреждения, не предусмотренные стандартом конструктивные изменения в архитектуре строения компьютера, его отдельных деталей (частей, блоков), особенно те, которые могли возникнуть в результате преступления, а равно могли спровоцировать возникновение происшествия;

– следы преступной деятельности (следы орудий взлома корпуса, проникновения внутрь корпуса, пальцев рук, несанкционированного подключения к компьютеру сторонних технических устройств и др.);

– расположение компьютера в пространстве, относительно периферийного оборудования и других электротехнических устройств;

– точный порядок соединения компьютера с другими техническими устройствами;

– категорию обрабатываемой информации (общего пользования или конфиденциальная);

– наличие или отсутствие индивидуальных средств защиты осматриваемого компьютера и обрабатываемой на нем информации от несанкционированного доступа и манипулирования.

Фотографирование и маркирование элементов компьютерной системы – важный первый шаг при подготовке системы к транспортировке. Доку-

---

[1] Бердникова О. П. Особенности первоначального и последующего этапа расследования мошенничества в сфере компьютерной информации. Екатеринбург : Уральский ЮИ МВД России, 2019. С. 26.

ментирование состояния системы на данном этапе необходимо для правильной сборки и подключения всех элементов системы в условиях лаборатории. При фотографировании следует исполнить снимки передней и задней частей системы крупным планом. Фотографирование и маркирование элементов изымаемой компьютерной техники дает возможность в точности воссоздать ее состояние в лабораторных условиях исследования. Некоторое оборудование типа внешних модемов может иметь множество мелких переключателей, фиксирующих его состояние, которые при транспортировке могут быть изменены, что создаст дополнительные проблемы для эксперта[1].

По делам о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, типичными местами производства обыска являются помещения (жилища), а также личный обыск подозреваемого (обвиняемого), который там находится[2].

По прибытии на место проведения обыска специфика действий будет состоять в следующем:

– определить места возможного отхода подозреваемого (обвиняемого) или выноса предметов и документов, имеющих значение для уголовного дела (запасный выход, окна и другие). Принять меры к установлению наблюдения за ними;

– быстро и внезапно войти в обыскиваемое помещение (жилище). Если их несколько – одновременно войти во все. На наш взгляд, нельзя согласиться с доводами отдельных авторов, полагающих, что в некоторых случаях, когда это возможно или целесообразно, непосредственно перед входом в обыскиваемое помещение следует обесточить его. Представляется, что при внезапном отключении электропитания в помещении (жилище) и наличии предположений у преступника о намерении сотрудников правоохранительных органов провести обыск, последним могут быть предприняты меры по уничтожению следов преступного посягательства. Таким образом, теряется не только фактор внезапности, но и ценные вещественные доказательства;

– в случае оказания активного сопротивления со стороны лиц, находящихся на объекте обыска, принять меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение (жилище);

– организовать охрану места обыска и наблюдение за ним. Охране подлежат: периметр обыскиваемых площадей; компьютерная техника; хранилища машинных носителей информации; все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади); специальные средства защиты от

---

[1] Сафронкина О. В., Шабаева Г. И. Особенности собирания следов преступления при расследовании мошенничества в сфере компьютерной информации // Право и государство: теория и практика. 2017. № 5 (149). С 142–144.

[2] Низаева С. Р. Цифровые следы. Виды, перспективы использования в целях раскрытия и расследования преступлений // Государственная служба и кадры. 2020. № 4. С. 187−194.

несанкционированного доступа; хранилища ключей (кодов, паролей) аварийного и регламентного доступа к компьютерной технике, помещениям и другим объектам, попавшим в зону обыска.

После реализации вышеуказанных мероприятий следователь должен перейти к обзорной стадии обыска и выполнить следующие действия:

– определить местонахождение подозреваемого (обвиняемого) на объекте обыска (если обыск осуществляется в его присутствии). При обнаружении – принять меры к отстранению его от пультов управления техническими устройствами, дистанцироваться от них и организовать охрану.

– определить и отключить специальные средства защиты информации и ЭВМ от несанкционированного доступа, особенно те, которые автоматически уничтожают компьютерную информацию и электронный носитель информации при нарушении процедуры доступа к ним, порядка их использования и (или) установленных правил работы с ними; принять меры к установлению пароля (кода) санкционированного доступа и ключа шифрования-дешифрования информации.

– установить наличие телекоммуникационной связи между компьютерами. При наличии компьютерной сети любого уровня технической организации осмотреть и обыскать управляющий сервер, который хранит в своей оперативной и постоянной памяти наибольшую часть компьютерной информации, управляет другими компьютерами, имеет с ними прямую и обратную связь. Следует учитывать, что у сообщников подозреваемого (обвиняемого) или у него самого (если обыск производится в его отсутствие) имеется возможность уничтожения искомой компьютерной информации дистанционно с помощью компьютеров, находящихся вне периметра обыскиваемой зоны.

– определить компьютеры, находящиеся во включенном состоянии, характер выполняемых ими операций. Внимание необходимо уделить печатающим и видеоотображающим устройствам. Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора – видеограмма изучена и детально описана в протоколе.

В заключение отметим, что при проведении следственных действий, связанных с расследованием преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий, целесообразно привлечь специалиста в области компьютерной техники и информации с момента проведения осмотра месте происшествия. До начала следственных действий следует также иметь данные о марке, модели компьютера, операционной системы, периферийных устройств, средств связи, и любые другие сведения о системе, которая является источником получения криминалистически значимой информации.

§ 4. Выявление и раскрытие преступлений, совершаемых с использованием информационно-коммуникационных технологий

4.1. Хищение денежных средств с банковских карт

Место начала совершения преступления – территория выхода абонентского номера преступника в эфир в момент поступления (согласно детализации телефонных звонков заявителя) СМС-сообщения заявителю или в момент разговора с последним, в ходе которых выполняются действия по обману потерпевшего.

Анализ практики раскрытия и расследования преступлений в сфере ИКТ показал, что следователи территориальных органов внутренних дел при возбуждении перед судами ходатайства в выносимых постановлениях не запрашивают исчерпывающий перечень информации, позволяющий впоследствии установить местонахождение преступника по месту выхода в эфир абонентского устройства (мобильного телефона с установленным абонентским номером, либо по установленному IMEI-номеру телефона).

Следует отметить, что для установления места нахождения преступника недостаточно получить информацию о номере и месте расположения приемопередающей базовой станции. Зачастую, наблюдаются случаи, что при «выходе в эфир» абонентского устройства, с которого злоумышленник совершает преступные действия, услуги связи оказываются через базовую станцию, расположенную на большем удалении, несмотря на наличие иных близлежащих приемопередающих базовых станций.

В постановлениях о возбуждении перед судом ходатайства в порядке, предусмотренном ст. 186.1 УПК РФ, о получении информации о соединениях между абонентами и (или) абонентским устройствами с привязкой к приемопередающим базовым станциям, необходимо конкретизировать запрашиваемую информацию: «Ходатайствовать перед судом о получении информации о соединениях между абонентами и (или) абонентским устройствами с привязкой к приемопередающим базовым станциям»[1].

После получения вышеуказанного постановления суда во исполнение ст. 6.1, ч. 2 ст. 21 УПК РФ, требующих принятия своевременных (наступательных) действенных мер по установлению события преступления, изобличению лица или лиц, виновных в совершении преступления, необходимо в течение суток после получения постановления суда, направить его с запросом (заверенным гербовой печатью) в порядке ч. 4 ст. 21 УПК РФ в компанию сотовой связи.

---

[1] Лакеева Е. В. Ходатайство о получении информации о соединениях между абонентами и (или) абонентскими устройствами: проблемные аспекты // Вестник Белгородского юридического института МВД России имени И. Д. Путилина. 2022. № 2. С. 49-53.

При наличии сведений о CID (номере приемопередающей базовой станции) и LAC (информации о зоне с неповторяющимися частотами, на которых излучает базовая станция) место расположения приемопередающей базовой станции возможно установить самостоятельно посредством бесплатного ресурса, размещенного в сети Интернет на сайте «Xinit.ru».

С целью получения исчерпывающей информации и раскрытия преступления (установления способа хищения и места нахождения преступника в момент изъятия из законного владения денежных средств), в постановлениях о возбуждении перед судом ходатайства в порядке, предусмотренном ст. 183 УПК РФ, о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях, необходимо конкретизировать запрашиваемую информацию.

После вынесения постановления суда о разрешении на получение данных сведений, во исполнение ст. 6.1, ч. 2 ст. 21 УПК РФ, требующих принятия своевременных (наступательных) действенных мер по установлению события преступления, изобличению лица или лиц, виновных в совершении преступления, необходимо в течение суток после получения постановления суда направить его с оформленным запросом (заверенным гербовой печатью) в порядке ч. 4 ст. 21 УПК РФ в отделение банка (по месту открытия счета (банковской карты) потерпевшего, с обязательным указанием разумных сроков исполнения постановления суда, разъяснением ответственности за невыполнение законных требований следователя, предусмотренной ст. 17.7 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ).

В связи с тем, что видеозаписи с камер наблюдения банкоматов сохраняются только в течение 60–90 суток, в запросе на имя службы безопасности банка необходимо указать на то, что при установлении мест обналичивания (снятия со счета) денежных средств, необходимо вместе с ответом предоставить записи с видеокамер банкомата, которые целесообразно изъять путем составления протокола осмотра места происшествия или выемки.

4.2. Хищение денежных средств с банковского счета с использованием социальных сетей

При расследовании уголовных дел о данных видах преступлений на первоначальном этапе с целью раскрытия преступления необходимо выполнить следующие действия:

– допросить заявителя (потерпевшего) по обстоятельствам совершения преступления, при этом выяснив дополнительно следующие вопросы:

1) имеется ли по месту его проживания персональный компьютер, ноутбук, планшет и Интернет-соединение (если да, то каким провайдером предоставляются услуги связи по выходу во всемирную сеть Интернет, под каким логином, паролем, MAC-адрес устройства);

2) кто кроме него имеет доступ к компьютеру, ноутбуку, планшету, иному устройству по выходу во всемирную сеть Интернет;

3) зарегистрирован ли он на сайте «Одноклассники»;

4) каковы его логин и пароль;

5) узнать идентификационный номер профиля заявителя на сайте «Одноклассники».

Работа с IP-адресами позволит получить информацию о «взломе» «Персональной страницы» пользователя социальной сети, «осуществлении факта несанкционированного доступа» к «Персональной странице».

Кроме того, в ходе допроса потерпевшего необходимо выяснить следующую информацию:

– кому известны реквизиты его банковской карты (номер на лицевой стороне, пин-код, номер на оборотной стороне карты (CVC), дата, до которой действительна карта);

– подключены ли у него услуги «Мобильный банк» и «Интернет-банк» (если да, то к какой сим-карте, с каким номером, у кого находится данная сим-карта, передавал ли он кому-либо данную сим-карту, терял ли её, восстанавливал);

– осуществлялся ли выход с персонального компьютера по его месту жительства на сайт «Одноклассники» иными лицами;

– осуществлял ли заявитель сам платежи в пользу данного сайта;

– имелись ли случаи санкционированного и несанкционированного удаленного доступа к его компьютеру (если да, то, когда и при каких обстоятельствах);

– оснащен ли компьютер заявителя (потерпевшего) программным обеспечением, препятствующим несанкционированному удаленному доступу (программами-брандмауэрами);

– какова модель его телефона;

– осуществлялся ли выход заявителем (потерпевшим) или иным лицом с телефона на сайт «Одноклассники» и каким образом (через поисковые браузеры или сразу путем перехода на сайт «Одноклассники», выяснить возможность выхода на сайты-клоны);

– какие программы и через какие браузеры были загружены заявителем в сотовый телефон и в какой период времени;

– оснащен ли сотовый телефон заявителя антивирусным программным обеспечением.

Допросить лиц, входящих в круг общения заявителя (потерпевшего), с целью установления их логинов и паролей доступа на сайте «Одноклассники» для обеспечения возможности последующей проверки проведения оплат в пользу названного сайта, а также установления возможных фактов передачи им банковской карты заявителем в предшествующие опросу периоды.

После получения необходимой информации, содержащей сведения об IP-адресах, установить компанию-провайдер через справочные Интернет-ресурсы. С целью получения исчерпывающей информации, раскрытия преступления (установления способа хищения и места нахождения преступника в момент изъятия из законного владения денежных средств) в порядке ст. 183 УПК РФ, выйти в суд с ходатайством о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях (получения информации о движении денежных средств по банковскому счету потерпевшего).

Произвести осмотр места происшествия – жилища заявителя с целью установления наличия либо отсутствия компьютеров, ноутбуков, планшетов, Интернет-соединений (установления MAC-адресов устройств соединений), провести осмотр изъятого системного блока компьютера (ноутбука, планшета) заявителя с участием специалиста в области информационных технологий, дать юридическую оценку его значимости.

4.3. Мошенничество, совершенное под предлогом сделки, связанной с куплей-продажей имущества через сеть Интернет

На первоначальном этапе с целью раскрытия преступления, необходимо выполнить следующие действия:

– изъять у заявителя (потерпевшего) и приобщить договор банковского счёта и документы об оформлении банковской карты (протоколом осмотра места происшествия, протоколом выемки);

– изъять у заявителя выписку из банковского счёта (протоколом осмотра места происшествия);

– допросить потерпевшего по обстоятельствам совершенного преступления, при этом выяснив ответы на следующие вопросы:

1) состав семьи, близкие родственники, лица, находящиеся на иждивении;

2) размер доходов и расходов потерпевшего по состоянию на момент совершения в отношении него преступления;

3) когда (дата, период времени) и на каком точно сайте, в какой социальной сети, в какой группе социальной сети он нашел объявление о продаже товара;

4) содержало ли объявление фотографические изображения продаваемого товара;

5) сохранились ли у потерпевшего фотографические изображения товара (при положительном ответе на указанный вопрос выемкой изъять, осмотреть, дать юридическую оценку значимости);

6) какие характеристики продаваемого товара были указаны в объявлении о продаже;

7) какие условия купли-продажи содержались в объявлении (условия о предоплате, оплате товара, сроках и видах поставки товара, ответственности сторон);

8) какие контактные данные продавца были указаны в объявлении о продаже;

9) имелись ли отзывы, комментарии к объявлению о продаже;

10) сохранились ли у него данные объявления (номер объявления, ID-страницы);

11) каким образом, когда (дата, время) потерпевший связался с продавцом;

12) как продавец представился потерпевшему (назвал ФИО, контактные данные, место своего нахождения, место нахождения товара);

13) попросить отразить подробное содержание разговора с продавцом;

14) что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю (потерпевшему) товара;

15) описание голоса продавца, сможет или нет его опознать (по каким приметам);

16) связывался ли потерпевший с продавцом посредством электронной почты; если да, то: установить адрес почтового ящика (аккаунта) потерпевшего, адрес почтового ящика (аккаунта) подозреваемого (продавца);

17) сохранились ли сообщения в его ящике электронной почты (если да, то: произвести выемку; в порядке ст. 186.1 УПК РФ выйти в суд с ходатайством о получении информации о лице, зарегистрировавшем почтовый ящик (аккаунт), содержании переписки за интересуемый период времени);

18) когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк он-лайн», «Мобильный банк»), в каком размере потерпевший перечислил на какой счет (номер счета, либо банковской карты, открытые на чье имя) денежные средства в счет оплаты за якобы приобретаемый товар;

19) если потерпевший осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк он-лайн», через «Личный кабинет», установить в ходе допроса место выхода потерпевшего в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, Wi-Fi роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в день хищения потерпевшему услуги связи по выходу в Интернет);

20) дата и место открытия счета (банковской карты), с которой потерпевший перечислил денежные средства;

21) каким образом известил «продавца товара» о перечислении денежных средств на указанную им банковскую карту (виртуальный кошелек);

22) что именно ему сообщил после подтверждения оплаты (перечисления денег на банковскую карту преступника) «продавец товара»;

23) в какой период времени, в какое место потерпевший прибыл для получения (как ему казалось) приобретенного товара;

24) когда он осознал, что в отношении него было совершено мошенничество, в результате которого похищены принадлежащие ему (иному владельцу) денежные средства;

25) является ли ущерб, причиненный потерпевшему от преступления для него значительным или нет.

Выемкой изъять у потерпевшего детализацию телефонных переговоров с его абонентского номера телефона за период с момента начала мошеннических действий до момента окончания. Произвести осмотр детализации телефонных переговоров потерпевшего, дать юридическую оценку значимости.

В случае установления факта использования преступником в ходе мошеннических действий сотового телефона, выйти в суд с ходатайством о получении информации о соединениях между абонентами и (или) абонентским устройствами с привязкой к приемопередающим базовым станциям.

После получения постановления суда, в соответствии со ст. 6.1, ч. 2 ст. 21 УПК РФ, в течение суток направить его с запросом в порядке ч. 4 ст. 21 УПК РФ в компанию сотовой связи, с обязательным указанием разумных сроков исполнения постановления суда, разъяснением ответственности за невыполнение законных требований следователя, предусмотренной ст. 17.7 Кодекс Российской Федерации об административных правонарушениях[1] (далее – КоАП РФ), а также ответственности по ст. 13.29 КоАП РФ, ст. 13.30 КоАП РФ.

Анализ практических исследований показал, что предпринимаемые меры по предупреждению преступлений в сфере информационных, коммуникационных, высоких технологий носят блочный характер, направлены на нейтрализацию отдельных угроз. Современные цифровые атаки связаны с действиями людей, их психологией поведения, шаблонными инструментами воздействия на пользователей.

В этой связи, мы убеждены, что эффективное противодействие преступлениям в сфере информационных, коммуникационных, высоких технологий базируется на основных системных алгоритмах:

I. Алгоритм анализа исследования закономерностей (характеристик) преступлений в сфере информационных, коммуникационных, высоких

---

[1] Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 декабря 2001 г. № 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

технологий: важно выявить их информативные особенности (маркеры), в том числе психологию поведения злоумышленника, его уязвимости.

II. Алгоритм реагирования на преступления в сфере информационных, коммуникационных, высоких технологий– необходимо обучение пользователей предупреждению, распознаванию атак, их своевременной фиксации (сохранению цифровых следов).

III. Алгоритм оперативного взаимодействия пользователей при выявлении преступлений в сфере информационных, коммуникационных, высоких технологий с правоохранительными органами; алгоритм оперативного взаимодействия правоохранительных органов (в том числе международного, межведомственного, внутриведомственного) с кредитными организациями, операторами сотовой связи, специалистами и др.

Выделим отдельные их значимые особенности.

I. По результатам исследования закономерностей преступлений в сфере информационных, коммуникационных, высоких технологий, выявлены отдельные значимые информативные их особенности (характеристики):

1. Личность злоумышленника. Характеризуется:

а) двумя группами лиц, находящихся в местах исполнения наказания за отдельные виды хищений, в том числе специализирующихся на цифровом мошенничестве, и всех остальных;

б) двумя базовыми акцентуациями характера: гипертимной, демонстративной (истероидной). Акцентуации характера злоумышленников образуют алгоритмизированный стереотип психологии их поведения при подготовке и совершении цифровых атак, выборе методов противодействия выявлению криминалистически значимой информации.

2. Личность пользователя (потерпевшего) характеризуется отсутствием у пользователя (потерпевшего) информации о личности злоумышленника, его психологии поведения, способах совершения преступлений в сфере информационных, коммуникационных, высоких технологий, способах сокрытия следовой картины цифровой атаки, методах их нейтрализации.

Социально-психологические характеристики пользователя (потерпевшего) отражают психологические черты, актуальные потребности, демографические характеристики, особенности когнитивных процессов, оценочное личностное отношение, способы поведения. Они же являются виктимологическими особенностями.

Личный опыт пользователя (например, особенности анализа объема исходящей информации, опыта столкновения с преступлениями в сфере информационных, коммуникационных, высоких технологий, знание основ информационной безопасности, умение распознавать индикаторы безопасности) влияет на возможность нейтрализации и предотвращения цифровых атак.

Психологическими векторами атаки являются следующие психологические реакции на кибератаки пользователей (потерпевших): невнимательность, любопытство, страх, раздражение, жадность, желание помочь. Важно отметить, что индуцируемые эмоции пользователей (потерпевших) в реализации цифровых атак явились и закономерностями психологии их поведения на манипулятивные техники злоумышленников. Это явилось квинтэссенцией выявления причин и условий, способствующих совершению преступлений в сфере информационных, коммуникационных, высоких технологий, с использованием социальной инженерии.

3. Обстановка, условия преступлений в сфере информационных, коммуникационных, высоких технологий характеризуется использованием сети Интернет (в социальных сетях, в интернет-магазинах, торговых интернет-ресурсах) и использованием средств мобильной телефонной связи, подключенных к сети Интернет (блокировка счета, банковской карты, незаконное списание денежных средств, маскировка хищений под видом социальных выплат, реализации социальных ресурсов и компенсаций).

Цифровые атаки осуществляются:

– по электронной почте, со ссылками и мошенническими страницами, например, вредоносные вложения, атаки по электронной почте с вложенными файлами;

– в социальных сетях (атаки злоумышленников на пользователей);

– через мобильные устройства: атаки злоумышленников по телефону, на смартфоны и мобильных пользователей;

– с использованием технологий искусственного интеллекта;

– в реальной жизни: цифровые атаки в физическом мире, например, пользуясь моментом, злоумышленники наносят цифровые атаки на теме COVID-19.

Модель противодействия преступлениям в сфере информационных, коммуникационных, высоких технологий реализуется через обнаружение и реагирование на цифровую атаку.

Внешний вид атаки характеризуется визуальным оформлением, узнаваемым авторитетным брендом, атрибуцией и персонификацией. Брендами, которыми прикрываются мошенники, являются известные российские банки, компании газовой, нефтяной отрасли. Мошеннические интернет-ресурсы представляют из себя страницу с красочным заголовком и ссылкой на видео с преимуществами проекта. В нижней части страницы – форма для сбора личных данных для последующего использования в рамках социальной инженерии.

4. Типовыми способами противодействия злоумышленников выявлению значимой информации явились следующие: выход в сеть злоумышленником из зоны Wi-Fi, изменение «МАК-адреса», выход в сеть через

подставные IP-адреса, уничтожение, фальсификация, утаивание следовой картины в информационной среде, в том числе, с использованием программных продуктов, и др.

II. Эффективными инструментами противодействия преступлениям в сфере информационных, коммуникационных, высоких технологий явились следующие меры:

1. Обучение и тренировка навыков пользователей с отработкой следующих вопросов:

– что они должны знать и уметь, какие навыки влияют на безопасность;

– как пользователи открывают письма и переходят по ссылкам (открывают вложенные файлы, вводят данные в формы, подключают съемные устройства);

– какие психологические и организационные векторы покрыты;

– что должны знать об объективных метриках безопасности;

– что делать при выявлении цифровых атак, алгоритм реагирования, особенности фиксации значимой информации;

– как обучить пользователей выявлению и предупреждению цифровых атак.

В этой связи интересен опыт Сбербанка России по обучению кибербезопасности своих клиентов. Так, например, клиенты Сбербанка России проходят курсы и сдают интерактивные тесты по вопросам безопасности; получают имитированные атаки по разным каналам и тренируют навыки: совершают или не совершают опасные действия, получают обратную связь. Статистика по обучению и тренировкам навыков поступает в антифрод-систему, как дополнительные метрики поведения по каждому клиенту.

Дополнительными метриками для антифрода по каждому обучающемуся являются: уровень знаний, навыков, опасные уязвимости программного обеспечения.

ФинЦЕРТ Сбербанка России рекомендует повышать киберграмотность населения, повышать качество работы операторов в области осведомления своих клиентов в вопросах киберграмотности, тренировать и измерять эти навыки с подготовкой системного отчета и дополнительного обучения по следующей формуле: знания и навыки с возможностью их измерения, корректировки с постоянной их тренировкой (знаний, умений, навыков).

2. Для предупреждения преступлений в сфере информационных, коммуникационных, высоких технологий специалисты в области IT-технологий и социальной инженерии рекомендуют усложнить злоумышленникам задачу:

– использовать VPN;

– шифровать всю конфиденциальную электронную корреспонденцию;

– использовать безопасный браузер;

– использовать безопасный IM-сервис с шифрованием;

– держать наготове вспомогательные VoIP-сервисы;

– использовать сервисы безопасного обмена сообщениями и переключаться между ними;

– обновлять программное обеспечение;

– при общении по мобильному устройству с предполагаемым злоумышленником достаточно задать ряд уточняющих вопросов, чтобы понять от кого на самом деле поступил звонок: фамилию, имя, отчество, должность, номер рабочего кабинета, рабочий телефон, просьбу прислать официальный документ в установленном порядке с необходимыми реквизитами. Основное предостережение: не сообщать по телефону свои персональные данные.

Использование системы «ПАК ИП-БЛК» и «Контур» для пресечения тюремных колл-центров также является эффективным инструментом для предупреждения преступлений в сфере информационных, коммуникационных, высоких технологий.

Учитывая, что не все инциденты могут быть первоначально распознаны или обнаружены, должны существовать процедуры для определения неудачных и удачных попыток нарушения кибербезопасности. В зависимости от масштабов ущерба, причиняемого конкретным инцидентом, может возникнуть необходимость в консультации экспертов для определения корневой причины инцидента, оценки эффективности реагирования и в случае ущерба для сохранения цепочек свидетельств − для судебного преследования преступника.

Понимание важности реагирования на преступления в сфере информационных, коммуникационных, высоких технологий и понимание влияния риска на безопасное функционирование информационной среды в случае появления угрозы в форме цифровых атак позволит предупреждать и нейтрализовать атаки в киберпространстве.

3. Ужесточение ответственности за противоправные посягательства в информационной сфере, совершенствование законодательной базы, развитие нормативной базы в этой области.

III. Типовыми алгоритмами явились следующие мероприятия: детализированный опрос (допрос) потерпевших, изъятие и осмотр средств мобильной связи и компьютерной техники, проведение отдельных сыскных мероприятий: наведение справок (направление запроса в необходимые кредитные организации, операторам сотовой связи, в специальные технические подразделения); снятие информации с технических каналов связи;

сбор образцов для сравнительного исследования, назначение и производство судебных экспертиз и иные мероприятия (оперативно-розыскные мероприятия и следственные (процессуальные) действия) позволят выявить и задокументировать криминалистически значимую информацию[1].

Исходя из вышеизложенного, необходимо отметить, что никакие комплексные технические средства защиты не помогут, если человек не будет самостоятельно осознавать серьезность кибератак, свое место и роль в выявлении, противодействии угрозам информационной безопасности.

[1] См. более подробно об этом: Лавров В. П. Исходные следственные ситуации и криминалистические методы их разрешения : сборник научных трудов / отв. ред. В. П. Лавров. М. : ВЮЗШ, 1991; Лавров В. П. Противодействие расследованию преступлений и меры по его преодолению : учебник / отв. ред. В. П. Лавров. М. : Академия управления МВД России, 2017; Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические, организационно-тактические и методические основы : дис. ... д-ра юрид. наук. М., 2009.; Гаврилин Ю. В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. № 4 (44). С. 45–50; Гаспарян Г. З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий : дис. ... канд. юрид. наук. М., 2020; Лонщакова А. Р. Возможность выявления криминалистически значимой информации при анализе реагирования на киберинциденты // Евразийский юридический журнал. 2021. № 2. С. 338–339.

ЗАКЛЮЧЕНИЕ

Взаимодействие следственных аппаратов с органами дознания способствует не только решению как общих, так и частных задач, стоящих перед ними, но и, что немаловажно, сближению этих задач, интеграции накопленных знаний, объединенных общей целью – борьба с преступностью.

Использование информационных-телекоммуникационных технологий, в частности, рассмотренного выше программного обеспечения в рамках проведения занятий по дисциплинам, связанным с приобретением навыков противодействия IT-преступности, позволят смоделировать максимально приближенные к реальным киберинцидентам условия, что приведет к формированию наиболее эффективной системы обучения и, соответственно, профессиональной адаптации к цифровой трансформации общества.

При проведении следственных действий, связанных с расследованием преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий, целесообразно привлечь специалиста в области компьютерной техники. До начала следственных действий следует также иметь данные о марке, модели компьютера, операционной системе, периферийных устройств, средств связи и любые другие сведения о системе, которая является источником получения криминалистически значимой информации.

Исходя из вышеизложенного, необходимо отметить, что никакие комплексные технические средства защиты не помогут, если человек не будет самостоятельно осознавать серьезность кибератак, свое место и роль в выявлении, противодействии угрозам информационной безопасности.

Для успешной работы в современной информационной среде от пользователей требуется не только знание интерфейсов программного обеспечения, но и понимание механизмов информационного обмена и взаимодействия их между собой, умение выявлять и исправлять ошибки в информационных базах. Систематизация понятий в этих сферах позволяет не только свободно ориентироваться в информационных системах, но и быть готовым к их изменениям.

Таким образом, данное учебное пособие позволит курсантам и слушателям, получить необходимые знания для эффективного выполнения профессиональных задач с использованием современных информационных технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты

1. **Российская Федерация. Законы.** Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 декабря 2001 г. № 195-ФЗ : текст с изменениями и дополнениями на 18 марта 2023 г. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 20.02.2023).

2. **Российская Федерация. Законы.** Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18 декабря 2001 г. № 174-ФЗ : текст с изменениями и дополнениями на 28 апреля 2023 г. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 10.05.2023).

3. **Российская Федерация. Законы.** О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 20.02.2023).

4. **Российская Федерация. Распряжения.** О подписании Конвенции о киберпреступности : распоряжение Президента Российской Федерации от 15 ноября 2005 г. № 557-рп // Собрание законодательства Российской Федерации. 2005. № 47. Ст. 4929. – Текст : непосредственный.

II. Учебная литература

1. **Аминев, Ф. Г.** Назначение и производство судебных экспертиз в расследовании преступлений / Ф. Г. Аминев, Л. С. Давлетшина, Э. Д. Нугаева. − Уфа : УЮИ МВД России, Уфа, 2007. – Текст : непосредственный.

2. **Бердникова, О. П.** Особенности первоначального и последующего этапа расследования мошенничества в сфере компьютерной информации. − Екатеринбург : Уральский ЮИ МВД России, 2019. – Текст : непосредственный.

3. Земельное законодательство: сборник документов / С. А. Боголюбов, О. А. Золотова. – Москва : Проспект, 2016. – Текст : непосредственный.

4. **Архипова, И. А.** Актуальные проблемы расследования преступлений в сфере компьютерной информации : сборник статей международной научно-практической конференции // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения). Москва, 2018. – Текст : непосредственный.

5. **Гаврилин, Ю. В.** Расследование преступлений, посягающих на информационную безопасность в экономической сфере: теоретические,

организационно-тактические и методические основы: дис. ... д-ра юрид. наук. Москва, 2009. – Текст : непосредственный

6. **Гаврилин, Ю. В.** Электронные носители информации в уголовном судопроизводстве – Текст : непосредственный // Труды Академии управления МВД России. − 2017. − № 4 (44).

7. **Гаспарян, Г. З.** Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: дис. ... канд. юрид. наук. Москва, 2020.– Текст : непосредственный

8. **Гридина, Ю. А.** Киберпреступность как новая криминальная угроза / Ю. А. Гридина, А. А. Русскова. – Текст : непосредственный // Интеллектуальные ресурсы – региональному развитию. – Ростов-на-Дону, 2019. – Т. 5. – № 2.

9. **Гукасян, А. А.** Методы киберкриминала / А. А. Гукасян. − Текст : непосредственный // Аллея науки. – Томск, 2018. – Т.2. – № 1 (17).

10. Ежемесячный сборник о состоянии преступности в России (2010 – 2020 гг.) // Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации [сайт]. – Текст : электронный. – 2021. – URL: http://crimestat.ru/analytics (дата обращения: 26.03.2023).

11. **Ишмеева, А. С.** Развитие цифровой экономики в современных условиях / А. С. Ишмеева, И. Н. Губайдуллина. − Текст : непосредственный // Форум. – 2022. – № 3 (26).

12. Конвенция о компьютерных преступлениях (Будапешт, 23.11.2001) // Совет Европы. – Текст : электронный. – URL: http://www.consultant.ru (дата обращения: 20.02.2023).

13. **Кырлан Марчел.** Правовое регулирование инвестиционной деятельности в банковской сфере : дис. ... канд. юрид. наук. – Москва, 2022. – Текст : электронный. − URL: https://vak.minobrnauki.gov.ru (дата обращения: 20.02.2023).

14. **Лавров, В. П.** Противодействие расследованию преступлений и меры по его преодолению : учебник / отв. ред. В. П. Лавров. − Москва : Академия Управления МВД России, 2017. – Текст : непосредственный.

15. **Лавров, В. П.** Исходные следственные ситуации и криминалистические методы их разрешения : сборник научных трудов / отв. ред. В. П. Лавров. – Москва : ВЮЗШ, 1991. – Текст : непосредственный.

16. **Лонщакова, А. Р.** Возможность выявления криминалистически значимой информации при анализе реагирования на киберинциденты. – Текст : непосредственный // Евразийский юридический журнал. − 2021. − № 2 (153).

17. **Лонщакова, А. Р.** Выявление криминалистически значимых маркеров при анализе уровней защиты информации. Отдельные особенности работы с группами риска – Текст : непосредственный // Проблемы раз-

вития современного общества : сборник научных статей 7-й Всероссийской национальной научно-практической конференции. − Курск, 2022.

18. **Низаева, С. Р.** Цифровые технологии в криминалистике. – Текст : непосредственный // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. − 2021. − № 21 (1).

19. **Низаева, С. Р.** Цифровые следы. Виды, перспективы использования в целях раскрытия и расследования преступлений. – Текст : непосредственный // Государственная служба и кадры. − 2020. − № 4.

20. **Нугаева, Э. Д.** Деловая игра – одна из форм эффективного метода обучения / Э. Д. Нугаева, С. М. Куценко – Текст : непосредственный // Вестник Уфимского юридического института МВД России. 2010. № 3.

21. Понятие киберпреступлений и методы защиты – Текст : электронный // Гражданская инициатива интернет политики [сайт]. – URL: https://internetpolicy.kg/literacymodule/course_2/module1/glava1_1.html (дата обращения: 26.03.2023).

22. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. Москва : Издательство Юрайт, 2022. – Текст : электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/496747 (дата обращения: 26.03.2023)

23. **Сафронкина, О. В.** Особенности собирания следов преступления при расследовании мошенничества в сфере компьютерной информации О. В.Сафронкина, Г. И. Шабаева. – Текст : непосредственный // Право и государство: теория и практика. − 2017. − № 5 (149).

24. **Смирнова, И. Г.** Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ : монография / И. Г. Смирнова и др. – Москва : Издательство Юрлитинформ, 2016. – Текст : непосредственный.

25. Советы по защите от киберпреступников – Текст : электронный // Лаборатории Касперского [сайт]. – URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 26.03.2023).

26. **Спиридонова, Н. Е.** Подходы к описанию динамики компьютерных преступлений / Н. Е. Спиридонова, В. В. Меньших // Информатика: проблемы, методология, технологии : сборник материалов XIX международной научно-методической конференции / под ред. Д. Н. Борисова. – Воронеж, 2019. – Текст : непосредственный.

27. **Сысенко, А. Р.** Особенности осмотра места происшествия при расследовании компьютерных преступлений / А. Р. Сысенко. – Текст : непосредственный // Закон и право. − 2020. − № 12.

28. **Тисен, П. А.** Противодействии вовлечению подростков в радикальные организации в Интернете / П. А. Тисен // II Всероссийская научно-практическая конференция «Новые, появляющиеся и видоизменяющиеся

формы преступности: научные основы противодействия (Долговские чтения)». – Ростов-на-Дону, 2022. – № 2. – Текст : электронный // Российская криминалистическая ассоциация им. А.И. Долговой [сайт]. – URL: http://crimas.ru/wp-content/uploads/2021/07/Maket-sbornika-materialov-Dolgovskie-chteniya-29.03.2021.pdf. (дата обращения: 26.03.2023)

29. **Цинделиани, И. А.** Финансовое право : учебник для бакалавров / И. А. Цинделиани. – Москва : Проспект, 2017. – Текст : непосредственный.

III. Источники на иностранных языках

1. Casey E., Thomas R. Digital transformation risk management in forensic science laboratories // Forensic Science International. V. 1. 2020.

2. Hamad B., Mishra A. Analysis of web browser for digital forensics investigation // International Journal of Computer Applications in Technology. V. 65 (2). 2021.

3. Paoli S., Johnstone J., Coull N., Ferguson I., Sinclair G., Tomkins P., Brown M., Martin R. A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists // Policing: A Journal of Policy and Practice. V. 15 (2). 2021.

Учебное издание

Гурьянова Венера Рафисовна
(кандидат физико-математических наук)
Тугузбаев Гаяз Ахтямович
(б/с, б/з)
Ишмеева Анастасия Сергеевна
(кандидат экономических наук, доцент)
и др.

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ОТДЕЛЬНЫЕ АСПЕКТЫ

Учебное пособие

Редактор *Е. А. Ермолаева*

Подписано в печать: 23.06.2023	Выход в свет: 29.06.2023
Гарнитура Times	Формат 60x84 1/16
Уч.-изд. л. 2,8	Усл. печ. л. 3
Тираж 100 экз.	Заказ № 30

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2