

Краснодарский университет МВД России

**Актуальные вопросы деятельности подразделений,
специализирующихся на предотвращении, выявлении,
раскрытии и расследовании преступлений,
совершаемых с использованием информационно-
коммуникационных технологий**

Учебное пособие

*Под общей редакцией доктора технических наук,
профессора О. М. Булгакова*

Краснодар
2023

УДК 343.2/.7
ББК 67.408.1
А437

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составители: *Е. В. Афанасьев, И. Г. Башинская, С. О. Бевз, А. Г. Бельный, Д. С. Богданов, О. М. Булгаков, Е. С. Бычкова, А. Н. Горбунов, М. М. Душенко, А. В. Еськов, Н. Н. Калинина, В. П. Легостаев, Ю. В. Лункашу, А. И. Макаренко, А. С. Победа, К. В. Протасов, А. А. Сафронов, В. В. Стукалов, А. А. Таганова, В. С. Южанинов, В. В. Яковлев.*

Рецензенты:

Н. В. Михайленко, кандидат юридических наук, доцент (Московский университет МВД России имени В.Я. Кикотя);

А. А. Бондарев, кандидат юридических наук, доцент (Орловский юридический институт МВД России имени В.В. Лукьянова).

Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий : учебное пособие / сост.: Е. В. Афанасьев, И. Г. Башинская, С. О. Бевз и др.; под ред. О. М. Булгакова. – Краснодар : Краснодарский университет МВД России, 2023. – 324 с.

ISBN 978-5-9266-1957-4

Рассматриваются вопросы деятельности подразделений органов внутренних дел, осуществляющих противодействие преступлениям, совершаемым с применением информационно-коммуникационных технологий. Содержатся темы, затрагивающие основы уголовного права, уголовного процесса, оперативно-розыскной деятельности органов внутренних дел, криминологии, экономической безопасности и другие.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.2/.7
ББК 67.408.1

ISBN 978-5-9266-1957-4

© Краснодарский университет
МВД России, 2023

Предисловие

Настоящее учебное пособие предназначено для профессионального обучения сотрудников полиции, проходящих службу в подразделениях органов внутренних дел, осуществляющих противодействие преступлениям, совершаемым с применением информационно-коммуникационных технологий. Компьютеризация базовых процессов жизнедеятельности, развитие и продвижение интернет-ресурсов, помимо очевидных благ для цивилизации, привели к криминализации интернет-пространства и широкому использованию информационно-коммуникационных технологий в качестве инструментов совершения преступлений. Рост количества преступлений, совершаемых с применением указанных технологий, совершенствование способов их совершения обусловили вовлечение в противодействие новому виду преступности сотрудников органов внутренних дел, обладающих широким спектром правоохранительных компетенций: следователей, дознавателей, экспертов-криминалистов, сотрудников уголовного розыска, подразделений специальных технических мероприятий.

В учебном пособии изложено содержание учебной дисциплины «Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий» в соответствии с ее примерной программой.

В данном учебном пособии охватывается широкая тематика, затрагивающая основы уголовного права, уголовного процесса, оперативно-розыскной деятельности органов внутренних дел, криминологии, информационных технологий, экономической безопасности, с высокой степенью взаимной интегрированности содержания многих тем. Освоение предлагаемого к изучению содержания требует от обучающихся широкого кругозора в области современных интернет-технологий и цифровизации информационных процессов, правоохранительной деятельности. В успешном освоении материала важную роль играет системный подход к организации не только аудиторных занятий образовательной программы профессионального обучения в целом, но и самостоятельной работы обучающихся, в данном случае обеспечивающей закрепление изученного материала, самостоятельное изучение отдельных вопросов, необходимый баланс общих и специальных знаний.

Учебная дисциплина «Актуальные вопросы деятельности подразделений, специализирующихся на предотвращении, выявлении, раскрытии и расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий» изучается в относительно небольшие сроки, поэтому в освоении ее содержания важная роль отводится учебной литературе, в частности базовому учебному пособию. В основу его разработки положена идея концентрированного и одновременно предельно широкого изложения содержания дисциплины как информационной основы проведения аудиторных занятий со всем многообразием современных средств наглядности, организации самостоятельной работы слушателей и их подготовки к промежуточной аттестации.

Для удобства самостоятельной работы слушателей в процессе обучения и подготовки к промежуточной аттестации содержание учебного пособия структурировано в соответствии с разделами и темами изучаемой учебной дисциплины, в тексте в формате подзаголовков воспроизведены формулировки дидактических единиц содержания. Стиль изложения и оформления – конспективный, лаконичный с использованием таблиц и схем, а также графических приемов концентрирования внимания читателя – выделения и обособления наиболее значимых понятий, определений и комментариев.

В конце каждой темы приведены примерные планы практических занятий и вопросы для самоконтроля, а в конце каждого раздела – списки литературы.

Учебное пособие можно использовать в качестве конспекта лекций или развернутого справочника, по текстовым фрагментам и смарт-объектам восстанавливая в памяти содержание интересующей темы.

В написании учебного пособия приняли участие: Афанасьев Е.В. (темы 3.3, 3.5, 3.7), Башинская И.Г. (темы 2.14, 3.1, 3.2, 3.4, 3.6), Бевз С.О. (тема 1.1), Белый А.Г. (темы 2.11, 2.13), Богданов Д.С. (тема 4.3), Булгаков О.М. (введение, темы 1.1, 2.8, 4.3), Бычкова Е.С. (тема 6.4), Данилов Д.Б. (темы 2.2, 2.9, 2.14), Еськов А.В. (тема 6.1.), Калинина Н.Н. (тема 6.2), Легостаев В.П. (темы 2.1, 2.4, 2.6), Лункашу Ю.В. (тема 1.5), Макаренко А.И. (тема 1.5), Победа А.С. (тема 5.2), Протасов К.В. (темы 5.5), Сафронов А.А. (темы 2.3, 2.7, 2.8, 4.1, 4.2, 5.1, 5.3, 5.4), Стукалов В.В. (темы 2.5, 2.15), Таганова А.А. (тема 6.3), Южанинов В.С. (темы 2.10, 2.12), Яковлев В.В. (темы 1.2, 1.3, 1.4, 1.6).

Принятые сокращения

БПС – базовая приемо-передающая станция;
ГК РФ – Гражданский Кодекс Российской Федерации;
ДБО – дистанционное банковское обслуживание;
ДОУ – дело оперативного учета;
ИК – информационная карта;
ИКТ – информационно-коммуникационные технологии,
информационно-телекоммуникационные технологии;
ИТКС – информационно-телекоммуникационная сеть;
КБС – контроллер базовой станции;
КПО – контроль почтовых отправлений, телеграфных и иных
сообщений;
КУСП – книга учета сообщений, преступлений
НПА – нормативный правовой акт;
НПС – национальная платежная система;
НСД – несанкционированный доступ;
ОВД – органы внутренних дел;
ОПП – оперативно-поисковые подразделения;
ОРД – оперативно-розыскная деятельность;
ОРМ – оперативно-розыскное мероприятие;
ОТМ – оперативно-техническое мероприятие;
ПКИ – получение компьютерной информации;
ПО – программное обеспечение;
ППРФ – постановление Правительства Российской Федерации;
ПСТМ – подразделение специальных технических мероприятий;
ПТП – прослушивание телефонных переговоров;
СВТ – средство вычислительной техники, средство электронно-
вычислительной техники;
СЗИ – средства защиты информации;
СОГ – следственно-оперативная группа;
УПРФ – Указ Президента Российской Федерации;
ФЗ – федеральный закон;
ФКЗ – федеральный конституционный закон;
ФТС – Федеральная таможенная служба;
ЦКПС – центр коммутации подвижной связи;
ЭКП – экспертно-криминалистическое подразделение;
ЭКУ – экспертно-криминалистические учеты;
ЭКЦ – экспертно-криминалистический центр.

1. ОБЩИЕ ПОЛОЖЕНИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Тема 1.1. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации

Правовое обеспечение процессов информатизации представляет совокупность нормативных правовых актов, принимаемых на различных уровнях власти и управления, регулирующих комплекс общественных отношений, связанных с созданием и использованием информации и перспективных информационных технологий¹.

В Конституции РФ информации посвящены следующие статьи:

Статья 24 ч. 1, в соответствии с которой «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются», и ч. 2, согласно которой «органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом»; статья 29 ч. 4, в соответствии с которой «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом», и ч. 5, согласно которой «гарантируется свобода массовой информации, цензура запрещается»; статья 71, согласно которой «в ведении Российской Федерации находятся... оборона и безопасность... обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных».

¹ Беляева Т.М. и др. Информационные технологии в юридической деятельности: учеб. / под ред. В. Д. Элькина. М.: Проспект, 2013.

*Конституционные положения, закрепляющие основные
информационные права и свободы, развиты и детализированы
в федеральном законодательстве*

ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ «Об информации»)	Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применение информационных технологий, обеспечение защиты информации
ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»	Регулирует отношения, связанные с обработкой государственными органами власти, юридическими и физическими лицами персональных данных, которые не составляют государственную тайну
Гражданский кодекс РФ	Осуществляет правовое регулирование создания и использования программ для ЭВМ и баз данных (ст. 1261, 1262, 1280, 1333, 1334, 1335, 1336)
Кодекс РФ об административных правонарушениях	Закрепляет ответственность за нарушение норм в сфере обработки персональных данных (ст. 5.39, 13.11, 13.12, 13.14)
Уголовный кодекс РФ	Определяет ответственность за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети и др. (ст. 137, 140, 272, 273, 274, 284, 292, 324)
ФЗ от 21 июля 1993 г. № 5485-1 «О государственной тайне»	регулирует отношения, возникающие в связи с отношением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации, определяет полномочия государственных органов и должностных лиц по обеспечению сохранности и защиты государственной тайны, содержит перечень сведений, составляющих государственную тайну
ФЗ от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»	Определяет принципы и способы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления, формы ее предоставления, права и обязанности пользователей информации, органов власти, их должностных лиц, устанавливает ответственность за нарушение порядка доступа к информации

Нормативные правовые акты, обеспечивающие правовое регулирование информационных отношений, возникающих в сфере внутренних дел, порядка применения информационных технологий и защиты информации в органах внутренних дел

ФЗ от 7 февраля 2011 г. № 3-ФЗ «О полиции».	Обязывает сотрудников ОМВД регулярно информировать государственные и муниципальные органы, граждан о своей деятельности через СМИ, информационно-телекоммуникационную сеть (ИТК) Интернет (п. 3 ст. 8)
УПРФ от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации»	Утвердил Положение о МВД России, в котором указано, что Министерство внутренних дел РФ формирует и ведет федеральные учеты, базы данных оперативно-справочной, розыскной, криминалистической, статистической и иной информации, а также использует в установленном порядке федеральные учеты, базы данных в этой области других федеральных органов исполнительной власти
ППРФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»	Установило требования по обеспечению защиты информации, содержащейся в информационных системах общего пользования
ППРФ от 24 мая 2010 г. № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов»	Утвердило Правила подготовки планов информатизации государственных органов, Правила проведения экспертной оценки документов, используемых в рамках планирования, создания и использования информационно-телекоммуникационных технологий (ИКТ) в деятельности государственных органов
ППРФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»	Определяет для государственных и муниципальных органов, обрабатывающих персональные данные, необходимость обязательного принятия ряда документов, обеспечивающих выполнение законодательства в области персональных данных
ППРФ от 25 апреля 2012 г. № 394 «О мерах по совершенствованию использования ИКТ в деятельности государственных органов»	Скорректированы акты Правительства РФ по вопросам совершенствования использования ИКТ в деятельности государственных органов

ППРФ от 6 сентября 2012 г. № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти»	Принят ряд мер по совершенствованию электронного документооборота в органах государственной власти, а также установлен срок (до 31 декабря 2017 г.) перехода к электронному взаимодействию федеральных органов исполнительной власти между собой и с Правительством РФ
ППРФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	Пересмотрены требования по защите персональных данных при их обработке в соответствующих информационных системах. За безопасность персональных данных отвечает оператор системы, который их обрабатывает, или уполномоченное им лицо. Оператор системы выбирает средства защиты информации в соответствии с нормативными актами ФСБ России и ФСТЭК России
ППРФ от 25 декабря 2014 г. № 1494 «Об утверждении правил обмена документами в электронном виде при организации информационного взаимодействия»	Определило правила обмена документами в электронном виде в органах государственной и исполнительной власти, местного самоуправления

Правовую основу реализации МВД России своих полномочий в сфере информатизации также составляют:

- Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»;
- Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
- Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»;
- Нормативные правовые акты МВД России, регулирующие вопросы развития информационных технологий, связи и защиты информации.

Во исполнение перечня поручений Президента РФ от 9 августа 2011 г. № Пр-2291 для информатизации служебной деятельности ОВД и предоставления государственных услуг создана Единая система информационно-аналитического обеспечения деятельности МВД России – ИСОД МВД России.

Сервисы ИСОД МВД России	
Общесистемные	Прикладные
СЭД, СУДИС, СЭП, ВИСП, СВКС-м, Форум, АПК «Официальный интернет-сайт МВД России»	СООП, СОМТО; ФИС ГИБДД-М, СЦУО, ЦИАДИС, СОДИ, СПГУ, СОПС, СОДЧ, СОКД, СОШП, СОДПП, СФП, Ксенон-2

Для организации защищенного доступа к сервисам ИСОД МВД России через проводные, спутниковые и беспроводные каналы связи назначены администраторы доступа, у которых пользователи получают единые учетные записи.

Одной из важнейших задач государства в области обеспечения защиты информации является создание и совершенствование сбалансированной системы правовых норм и механизмов, направленных на противодействие и нейтрализацию угроз государственным интересам России в этой сфере.

Объект правового регулирования в области защиты информации – отношения между органами законодательной, исполнительной и судебной власти, органами местного самоуправления, предприятиями, учреждениями и организациями, должностными лицами и гражданами Российской Федерации по поводу реализации своих прав и обязанностей относительно предметов правовых отношений при исполнении ими требований законодательства о защите информации.

Предмет правовых отношений в области защиты информации – информация, информационные ресурсы, информационные технологии и средства обработки информации.

Государственное регулирование отношений в данной сфере осуществляется путем установления требований к защите информации и установления ответственности за нарушение законодательства Российской Федерации о защите информации.

Оператор обязан обеспечивать защиту всей информации, которая обрабатывается в информационных системах и содержится в базах данных.

ИНФОРМАЦИЯ		
Общедоступная	Ограниченного доступа	
	сведения, составляющие государственную тайну: «секретно», «совершенно секретно», «особой важности»	конфиденциальная информация

Ограничение доступа к информации устанавливается Конституцией РФ и федеральными законами.

Деятельность предприятий, учреждений и организаций по выполнению работ и оказанию услуг по защите государственной тайны или созданию средств защиты информации (СЗИ) требует получения ими лицензий на проведение работ со сведениями соответствующей степени секретности¹. Законодательная база лицензирования: закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» и Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Порядок получения лицензий устанавливается Правительством РФ. Соответствующее лицензирование осуществляют органы, определенные Правительством РФ: ФСБ России и ее территориальные органы (на территории Российской Федерации) и СВР России (за рубежом).

Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»² определены особенности технического регулирования в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа.

Техническое регулирование – установление и соблюдение технических норм и правил подтверждения соответствия продукции, процессов проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, работ, услуг требованиям технических регламентов (стандартов, сводов правил или договоров), а также государственного контроля (надзора) за соблюдением таких требований.

Наряду с требованиями технических регламентов в отношении указанной продукции (работ, услуг) и соответствующих процессов обязательные требования устанавливаются:

– федеральными органами исполнительной власти – ФСБ России³, Минобороны России⁴, СВР России⁵, ФСТЭК России⁶;

¹ О государственной тайне: закон от 21.07.1993 № 5485-1 // Собр. законодательства РФ. 1997. № 41. стр. 8220–8235.

² О техническом регулировании: федер. закон РФ от 27.12.2002 № 184-ФЗ // Собр. законодательства РФ. 2002. № 52. Ч. 1. Ст. 5140.

³ Вопросы федеральной службы безопасности Российской Федерации: указ Президента РФ от 11.08.2003 № 960 // Собр. законодательства РФ. 2003. № 33. Ст. 3254.

⁴ Вопросы Министерства обороны Российской Федерации: указ Президента РФ от 16.08.2004 № 1082 // Собр. законодательства РФ. 2004. № 34. Ст. 3538.

⁵ О внешней разведке: федер. закон от 10.01.1996 № 5-ФЗ // Собр. законодательства РФ. 1996. № 3. Ст. 143.

⁶ Вопросы Федеральной службы по техническому и экспортному контролю: Указ Президента РФ от 16 августа 2004 г. № 1085 // СЗ РФ. 2004. № 34. Ст. 3541.

– государственными заказчиками (в контрактах, договорах).

Средства защиты информации подлежат обязательной сертификации уполномоченными федеральными органами – ФСТЭК России, ФСБ России и Минобороны России, т. е. подтверждению их соответствия требованиям по защите сведений соответствующей степени секретности с оформлением удостоверяющего сертификата. Срок действия сертификата не может превышать пяти лет. Координацию работ по организации сертификации средств защиты информации осуществляет межведомственная комиссия по защите государственной тайны.

В Госстандарте России зарегистрированы Система сертификации средств защиты информации по требованиям безопасности информации РОСС.RU.0001.01БИ00 и Система сертификации средств криптографической защиты информации РОСС.RU.0001.030001, определяющие организацию и основные правила сертификации СЗИ и шифровальных средств. Федеральные органы сертификации создают и собственные системы сертификации¹, в частности СЗИ-ГТ², устанавливая виды подлежащих сертификации СЗИ, порядок их испытаний и контроля.

Перечень СЗИ, подлежащих сертификации в системах сертификации РОСС.RU.0001.01БИ00 и СЗИ-ГТ, определены в нормативных правовых актах ФСТЭК России и ФСБ России соответственно.

Правовые отношения по созданию, преобразованию и потреблению информации в любых отраслях и направлениях деятельности подпадают под правовое регулирования нормами информационного права.

Информационное право – совокупность правовых норм, регулирующих отношения, связанные с информацией, т. е. деятельность субъектов права в информационной сфере.

¹ О государственной тайне: закон РФ от 21.07.1993 № 5485-1 // Собр. законодательства РФ. 1997. № 41.

² Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия: приказ ФСБ РФ от 13.11.1999 № 564. Доступ из справ.-правовой системы «Гарант».

Система информационного права	
Общая часть	Особенная часть
Основные понятия, общие принципы, правовые формы и методы правового регулирования деятельности в информационной сфере, содержание предмета и метода правового регулирования информационных отношений, характеристика источника информационного права	Институты информационного права, содержащие нормы, регулирующие общественные отношения по поводу обращения открытой, общедоступной информации: интеллектуальной собственности применительно к информационным объектам, массовой информации, библиотечного дела, архивного дела
Правовое регулирование отношений: при осуществлении права на поиск, получение и использование информации; при самостоятельном обороте информации; при обращении документированной информации; при установлении правового режима информационных технологий и средств их обеспечения; информационной безопасности. Правовые проблемы Интернета как виртуальной информационной сферы.	Институты информации ограниченного доступа: государственной тайны, служебной тайны, коммерческой тайны, банковской тайны, персональных данных и т. п.

Правовой институт – это совокупности правовых норм, регулирующих однородные общественные отношения определенной узкой области внутри отрасли (подотрасли) права.

Информационное право активно использует основные положения теории государства и права, взаимодействует с такими отраслями, как конституционное право, административное право, финансовое право, уголовное право, гражданское право, трудовое право, судостроительство, международное публичное и частное право.

Информационное право основано на конституционных нормах. Конституционное право закрепляет основные права и свободы личности, в том числе информационные права и свободы, закрепляет общие основы организации и деятельности представительных и исполнительных органов власти. Информационное право распространяется на оба этих вида государственной деятельности, поскольку информационная деятельность осуществляется и теми, и другими органами.

Информационное право активно использует методы административного права, в первую очередь при регулировании отношений, возникающих при осуществлении органами государственной власти и местного самоуправления обязанностей в области массовой информации: по формированию информационных ресурсов и предоставлению информации из них гражданам и юридическим лицам. Информационное право использует административно-правовые нормы при установлении ответственности за правонарушения в информационной сфере, регулировании деятельности субъектов в данной сфере, в том числе лицензировании информационных продуктов и информационных ресурсов. Во взаимодействии с административным правом информационное право регулирует общественные отношения при обороте информации ограниченного доступа.

Информационное право взаимодействует с уголовным правом, которое устанавливает ответственность за преступления в информационной сфере при нарушении норм информационного законодательства.

Связь информационного и гражданского права проявляется при регулировании имущественных отношений и личных неимущественных отношений по поводу информации и информационных объектов в информационной сфере, например, интеллектуальной собственности.

Гражданская правоспособность в информационной сфере – признаваемая государством за гражданами возможность иметь гражданские права и нести гражданские обязанности в информационной сфере. Субъектами правоотношений здесь выступают физические и юридические лица, а также органы государственной власти и местного самоуправления, которые вступают между собой в гражданско-правовые отношения в информационной сфере.

Орган государственной власти или местного самоуправления, юридическое или физическое лицо, которые могут быть участниками регулируемых нормами информационного права общественных отношений, являются субъектами информационного права. Чтобы выступать в роли такого субъекта необходимо обладать информационной правосубъектностью, которая складывается из информационной правоспособности и информационной дееспособности.

Информационная правоспособность – определяемая информационно-правовыми нормами возможность или способность данного субъекта вступать в правовые отношения в информационной сфере, т. е. приобретать в данной сфере права и обязанности и нести юридическую ответственность за их практическую реализацию.

Правоспособность субъекта является предпосылкой возникновения правовых отношений с его участием.

Информационная дееспособность – практическая способность субъекта своими действиями реализовать свою информационную правоспособность (права, интересы, обязанности, ответственность) в условиях конкретных информационных правоотношений.

Основные категории субъектов, действующих в информационной сфере:

- производители информации, информационных ресурсов, информационных продуктов, информационных услуг, а также информационных систем, технологий и средств их обеспечения;
- обладатели информации, информационных ресурсов, информационных продуктов, собственники информационных систем и средств их обеспечения;
- потребители информации, информационных ресурсов, информационных продуктов, информационных услуг.

Важнейшим субъектом информационного права является государство, которое как собственник основных информационных ресурсов и технологий обеспечивает единое информационное пространство страны, формирует ее информационную политику, в том числе в международной информационной сфере. Для органов государственной власти и местного самоуправления участие в информационных правоотношениях – прямая юридическая обязанность, главное средство практической реализации установленной для них компетенции – обязанности по информационному обеспечению физических и юридических лиц, а отсюда и правоспособности.

Юридические лица в информационной сфере (предприятия и учреждения: создатели и распорядители информационных ресурсов, поставщики информационных услуг, СМИ, архивы, библиотеки, спецхраны, банки, культурные фонды и др.) реализуют свою информационную дееспособность через своих руководителей, коллективные органы управления, учредителей.

Для всех субъектов, действующих в информационной сфере, устанавливается гражданско-правовая, административно-правовая и уголовная ответственность за неправомерное поведение.

Рассмотрим основные термины и определения правовых понятий в области информационных отношений и защиты информации, установленные в ФЗ «Об информации».

Информация – сведения (сообщения, данные) независимо от формы их представления

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система – это система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

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

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

обладателями (собственниками) информации могут быть государство, организации (юридические лица) и граждане

Доступ к информации – возможность получения информации и ее использования.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Электронное сообщение – информация, переданная или полученная пользователем ИТКС.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Электронный документ – документированная информация, представленная в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по ИТКС или обработки в информационных системах.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Сайт в сети Интернет – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством ИТКС Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в Интернете.

Страница сайта в сети Интернет (интернет-страница) – часть сайта в интернете, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта.

Доменное имя – обозначение символами, предназначенное для адресации сайтов в интернете в целях обеспечения доступа к информации, размещенной в интернете.

Сетевой адрес – идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему.

Владелец сайта в сети Интернет – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в интернете, в том числе порядок размещения информации на таком сайте.

Провайдер хостинга – лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к интернету.

Единая система идентификации и аутентификации – федеральная государственная информационная система, порядок использования которой устанавливается Правительством РФ и которая обеспечивает в случаях, предусмотренных законодательством российской федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Поисковая система – информационная система, осуществляющая по запросу пользователя поиск в Интернете информации опреде-

ленного содержания и предоставляющая пользователю сведения об указателе страницы сайта в Интернете для доступа к запрашиваемой информации, расположенной на сайтах в Интернете, принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

Идентификация – совокупность мероприятий по установлению сведений о лице и сопоставлению данных сведений с необходимым для определения такого лица уникальным отображением сведений о нем (идентификатором).

При идентификации (от позднелатинского *identifico* – отождествляю) решение сводится к выбору того идентификатора из их общей совокупности, хранящихся в системе, который наиболее близок к предъявляемым сведениям о лице, или к признанию лица неидентифицируемым. Примеры идентификации: введение логина пользователем информационного ресурса и его распознавание, считывание кода прокси-карты при прохождении турникета.

Аутентификация – совокупность мероприятий по проверке лица на принадлежность ему идентификатора посредством сопоставления идентификатора со сведениями о лице, которыми располагает субъект, проводящий аутентификацию, и установлению правомерности владения лицом идентификатором, в результате чего лицо считается установленным.

Примеры аутентификации: введение пароля пользователем информационного ресурса и его распознавание, проверка дежурным служебного удостоверения сотрудника.

Рассмотрим основные понятия в области защиты информации на основе ГОСТ Р 50922-96, руководящих документов Гостехкомиссии России и научных публикаций.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, установленными правовыми документами или собственником информации.

Защита информации – принятие правовых, организационных и технических мер, направленных:

– на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования,

предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Защита информации от несанкционированного доступа (НСД) – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правил доступа к защищаемой информации.

Защита информации от разглашения – деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и НСД.

Защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее модификации, уничтожению, хищению, блокированию доступа.

Защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя в работе технических и программных средств информационных систем, природных и техногенных явлений или иных нецеленаправленных на изменение информации факторов, приводящих к ее модификации, уничтожению, хищению, блокированию доступа.

Защита информации от разведки – деятельность, направленная на предотвращение получения защищаемой информации разведкой (технической, агентурной).

Цель защиты информации – предотвращение ущерба для обладателя информации или ее пользователя в результате возможной утечки информации или несанкционированного и непреднамеренного воздействия на нее.

Эффективность защиты информации – степень соответствия результатов защиты информации поставленной цели.

Нормы эффективности защиты информации – значения показателей эффективности защиты информации, установленные нормативными документами.

Организация защиты информации – содержание и порядок действий, направленных на обеспечение защиты информации.

Система защиты информации – совокупность субъектов, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Объект защиты информации – подлежащая защите информация или носитель информации, или информационный процесс.

Мероприятие по защите информации – совокупность действий, направленных на разработку и применение способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации – совокупность действий, направленных на разработку и применение способов и средств контроля эффективности защиты информации.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Категорирование защищаемой информации (объекта защиты) – установление градации важности защищаемой информации (объекта защиты).

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и нормам.

Основные понятия, связанные с защитой информации в информационных системах, определены также в руководящем документе Гостехкомиссии «Термины и определения в области защиты от несанкционированного доступа к информации».

Установленные термины обязательны для применения во всех видах документации. Использование их смысловых эквивалентов не допускается.

Интернет – глобальная сетевая автоматизированная информационная система, состоящая из трансграничных ИТКС и распределенных в них информационных ресурсов, в их совокупности представляющая собой интегральный источник знаний и средство комму-

никации и информационного обмена, основу формирования и развития информационного общества.

Интернет нередко рассматривают как новую информационную жизненную среду человечества, деятельности личности, общества и государства, полагая ее виртуальной в противоположность реальной среде обитания – биосфере.

По признаку наличия государственно-властного элемента можно выделить следующие виды информационных правоотношений в Интернете: публично-правовые и частноправовые отношения.

Можно выделить следующие публично-правовые отношения в Интернете:

- отношения, возникающие при функционировании «электронного правительства» – системы, при которой права граждан на оказание им публичных услуг реализуются органами государства с помощью глобальных компьютерных сетей;
- отношения по лицензированию деятельности провайдеров, удостоверяющих центров и иных субъектов, по регистрации электронных СМИ и сертификации технических средств;
- отношения по привлечению к ответственности за преступления и правонарушения, совершенные с использованием Интернета;
- отношения в сфере электронной коммерции (типа Business to Administration, B2A).

Поскольку в данных отношениях одной стороной является государственный орган, на них распространяется принцип «все, что не разрешено, запрещено». Так как все государственные властные функции осуществляются исключительно на основе законодательства, то публично-правовые информационные отношения подлежат регулированию только «сверху», правом.

Например, для функционирования электронного правительства должен быть детально разработан его регламент, закреплены права и гарантии граждан.

Все остальные отношения, в которых отсутствует государственно-властный элемент, можно назвать частноправовыми интернет-отношениями, и здесь необходим совсем другой подход к выбору методов правового регулирования, которые должны обеспечить баланс частных и общественных интересов. Интернет составляет основу формирования и развития информационного общества, которое по своей политической сути является гражданским, и в нем должен действовать принцип «все, что не запрещено, разрешено».

Субъекты Интернета

1. Субъекты, которые создают программно-техническую часть информационной инфраструктуры Интернета, обеспечивают ее эксплуатацию, расширение и развитие. Это разработчики трансграничных информационных сетей, средств телекоммуникаций, технических и программных средств.

2. Субъекты, которые производят и распространяют информацию в Интернете, создают информационные ресурсы и делают их доступными потребителям, предоставляют услуги по подключению к сети.

3. Потребители информации и услуг в Интернете:

- потребители информации в Интернете;
- потребители хостинга, т. е. услуг по размещению информации на интернет-серверах;
- потребители услуг электронной почты.

Основные объекты информационных отношений в Интернете:

- программно-технические комплексы, информационные системы, ИКТ как средство формирования информационной инфраструктуры, средства связи и телекоммуникаций, обеспечивающие осуществление информационных процессов;
- информация, информационные ресурсы, информационные продукты, информационные услуги;
- доменные имена;
- информационные права и свободы;
- интересы личности, общества, государства в информационной сфере;
- информационная целостность и информационный суверенитет государства;
- информационная безопасность.

Интернет сам по себе не является ни субъектом, ни объектом права. Это техническое средство передачи и размещения информации, информационная среда, в которой складываются определенные отношения, часть которых является правоотношениями. Эти правоотношения носят информационный характер, поэтому их правовое регулирование опирается на действующие нормы информационного законодательства.

Вопросы для самостоятельного изучения

1. Полное наименование и назначение сервисов ИСОД МВД России.
2. Понятие технического регламента, стандарта.
3. Сущность отношений типа Business to Administration.

Примерный план занятия

1. Нормативные правовые акты, регулирующие общественные отношения в сфере информации, информационных технологий и защиты информации.
2. Отрасли права, регламентирующие отношения, возникающие при формировании и использовании информационных ресурсов.
3. Субъекты информационного права.
4. Основные термины и понятия в сфере информатизации.
5. Государственная политика в области защиты информации. Основные термины и понятия информационной безопасности.
6. Субъекты и объекты правоотношений в Интернете как глобальной информационно-коммуникационной сети.

Вопросы для самоконтроля по теме

1. В каких статьях Конституции Российской Федерации нашли отражение права граждан в информационной сфере?
2. Что составляет правовую основу деятельности МВД России в информационной сфере?
3. Что включают в себя общая и особенная части информационного права?
4. Что называют информационной правосубъектностью?
5. Как структурируется информация по степени доступности?
6. Какие государственные структуры реализуют государственную политику в области информационной безопасности? Каким образом они осуществляют контроль выполнения требований законодательства Российской Федерации субъектами информационных отношений?
7. Какая деятельность в Интернете определяется как публично-правовые отношения?
8. Кто является субъектом информационных отношений в Интернете?

Тема 1.2. Уголовно-правовая характеристика и квалификация преступлений, совершаемых с использованием информационно-коммуникационных технологий

Развитие современного информационного общества связано с интенсификацией процессов создания, обработки и хранения информации, использования информационных потоков во всех сферах социальной жизни. В настоящий момент темпы развития человечества определяются объемом доступной ему информации.

Информационная сфера активно осваивается криминальными структурами, создающими реальную угрозу национальным интересам Российской Федерации. Освоение преступным миром киберпространства осуществляется по двум основным направлениям, определяющим содержание и направленность преступной деятельности:

Посягательства на информационную безопасность общества и государства, где предметом выступает компьютерная информация; средства ее хранения, обработки и передачи; ИКТ; критическая информационная инфраструктура Российской Федерации	Посягательства на объекты уголовно-правовой охраны, не относящиеся к сфере компьютерной информации (представлены в разделе «Сведения о преступлениях, совершенных с использованием ИКТ» статистического сборника ГИАЦ МВД России)

Компьютерное преступление (преступление с использованием компьютера) представляет собой любое уголовно наказуемое деяние, затрагивающее автоматизированную обработку данных или передачу данных. При этом компьютерная информация является предметом или средством совершения преступления.

Киберпреступление – акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет¹.

Уголовно-правовое определение компьютерной информации законодательно закреплено в примечании 1 к ст. 272 УК РФ: «...Сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки, и

¹ Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 163.

передачи». Другими словами, под уголовно-правовой защитой находится не только информация, зафиксированная на каком-либо носителе, но и находящаяся в процессе передачи.

Компьютерная информация как объект правовых отношений регламентируется ФЗ «Об информации». В ст. 5 данного нормативного источника закреплено, что информация может являться объектом публичных, гражданских и иных правовых отношений. **Информация, в зависимости от порядка ее предоставления или распространения, подразделяется:**

- на информацию, свободно распространяемую;
- предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Виды охраняемой законом информации

информация, составляющая государственную тайну, режим защиты которой устанавливается федеральным законом
конфиденциальная информация, режим защиты устанавливается в основном собственником или владельцем на основании закона, а в ряде случаев федеральным законом
документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

Состав преступлений, совершаемых с использованием ИКТ.

Правовое регулирование преступлений в сфере компьютерной информации в УК РФ осуществлено путем закрепления в гл. 28 «Преступления в сфере компьютерной информации» четырех составов:

- 1) неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- 2) создание, использование и распространение вредоносных компьютерных программ для ЭВМ (ст. 273 УК РФ);
- 3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-компьютерных сетей (ст. 274 УК РФ);
- 4) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Общественная опасность преступлений в сфере компьютерной информации: неправомерный доступ или изменение компьютерной информации может нарушать деятельность различных систем обеспечения государства (обороны, энергетики, транспорта) и повлечь не только материальный ущерб, но и человеческие жертвы.

Объект преступления в сфере ИКТ

Родовой объект	Совокупность общественных отношений в сфере обеспечения общественной безопасности
Видовой объект	Общественные отношения в сфере обеспечения безопасности компьютерной информации
Непосредственный объект	Определяется исходя из названий и содержания диспозиций конкретных статей
Дополнительный объект	неприкосновенность частной жизни; права и свободы личности; имущественные интересы; основы конституционного строя; государственная безопасность

Предметом преступления в сфере ИКТ является непосредственно компьютерная информация.

Объективная сторона преступления в сфере ИКТ

Общественно опасное деяние	В основном деяния совершаются путем активного поведения человека. Однако нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-компьютерных сетей (ст. 274 УК РФ) возможно также путем бездействия
Общественно-опасные последствия	Присутствует в большинстве составов преступлений, находящихся в гл. 28 УК РФ
Причинно-следственная связь между деянием и последствиями	

Субъект преступления в сфере ИКТ во всех рассматриваемых составах общий – вменяемое физическое лицо, достигшее возраста наступления уголовной ответственности (16 лет).

Субъективная сторона преступления в сфере ИКТ

Субъективная сторона рассматриваемых деяний может характеризоваться как умышленной, так и неосторожной формами вины. Среди мотивов, характерных для всех компьютерных преступлений, преобладают два основных: корысть и «интеллектуальный вызов», т. е. стремление продемонстрировать собственный профессионализм. Во втором случае речь идет о ином личном мотиве

Проблемы правоприменительной практики при квалификации преступлений, совершенных с использованием ИКТ. В ст. 272 УК РФ законодатель соединил в одном составе несколько деяний, являющихся самостоятельными преступлениями в зарубежном уголовном законодательстве. Речь идет о незаконном доступе к компьютеру (компьютерной системе) и вмешательстве в систему или данные (ст. 2, 4 и 5 Конвенции о киберпреступности). Еще до принятия Конвенции некоторые зарубежные страны разграничили три указанных преступления.

В частности, ответственность за незаконный доступ предусмотрена в ст. 138а УК Голландии и ст. 197 УК Испании в главе против преступлений, посягающих на общественный порядок и неприкосновенность частной жизни; случаи вмешательства в систему (Интеллектуального (компьютерного) саботажа по УК Голландии) по голландскому УК и УК Испании отнесены к главе о причинении вреда.

Многие лица, получающие доступ к компьютерным системам и сетям, убеждены, что они не делают ничего противозаконного и уголовно наказуемого (а если исходить из действующего уголовного кодекса, то так оно и есть), даже если им приходится нарушать системы защиты, установленные пользователем. Однако для нормального функционирования компьютерных систем и обеспечения безопасности хранения и передачи информации уголовный закон должен защищать компьютер любого пользователя, пользующегося средствами защиты. Поэтому во многих зарубежных правовых порядках незаконный доступ к компьютеру приравнивается к незаконному проникновению в жилище, поскольку в обоих случаях преступник посягает на конституционные права граждан: на неприкосновенность жилища (ст. 25 Конституции РФ) и неприкосновенность частной жизни, личную и семейную тайну (ч. 1 ст. 23 Конституции РФ). Такой подход представляется оправданным, учитывая роль компьютеров в жизни современного человека, когда в нем может храниться большой объем сведений о человеке, касающихся разных сфер его жизни.

Примерный план занятия

1. Особенности уголовно-правовой квалификации преступлений, совершаемых с использованием ИКТ. Содержание и соотношение понятий «преступления в сфере компьютерной информации», «преступления, совершаемые с использованием современных ИКТ», «компьютерные преступления», «киберпреступления», «преступления в сфере информационных технологий».

2. Понятие компьютерной информации.
3. Компьютерная информация как объект правовых отношений.
4. Виды охраняемой законом компьютерной информации.
5. Юридические признаки и свойства компьютерной информации.
6. Состав преступлений, совершаемых с использованием ИКТ.

Вопросы для самоконтроля по теме

1. Чем обусловлена необходимость закрепления в уголовном законе составов преступлений, посягающих на компьютерную информацию?
2. Перечислите виды компьютерной информации, охраняемой уголовным законом.
3. Перечислите наиболее важные факультативные объекты преступлений в сфере ИКТ.
4. Назовите специфические черты объективной стороны преступления в сфере ИКТ.
5. Каковы наиболее характерные мотивы совершения преступлений в сфере ИКТ?
6. Назовите признаки субъекта преступления в сфере ИКТ.

Тема 1.3. Криминалистическая и криминологическая характеристики преступлений, совершаемых с использованием информационно-коммуникационных технологий

Понятие и состав криминалистической характеристики преступлений, совершаемых с использованием компьютерной информации. Криминалистическая характеристика преступлений представляет собой устойчивую и динамически развивающуюся систему, включающую в себя определенный, характерный только для нее набор элементов (присущий конкретному составу), знания о которых помогают выявить и расследовать деяние; составляющие ее элементы находятся в тесной корреляционной связи и зависимости друг с другом.

Элементный состав криминалистической характеристики преступлений, совершаемых с использованием компьютерной информации	
Характеристика предмета преступного посягательства	Характеристика способа преступления как троичная система, включающая способ подготовки, совершения и сокрытия
Характеристика материальных и идеальных следов преступления (механизм следообразования)	Характеристика основных обстоятельств преступления (место, время, обстановка)
Характеристика личности преступника с учетом целей и мотивов совершения преступления	

Наиболее распространенные способы совершения преступлений с использованием сети Интернет. Наиболее значимым элементом криминалистической характеристики преступлений, совершаемых с использованием ИКТ, является способ преступления, представляющий собой тройственную систему: подготовка, совершение, сокрытие. Рассматриваемые способы могут быть сгруппированы, в виде подготовки и совершения, совершения и сокрытия, подготовки и сокрытия. Способ совершения преступлений с использованием ИКТ может быть классифицирован по нескольким основаниям.

В зависимости от использования информационных ресурсов и характера преступных действий:	
Фишинг – массовая рассылка сообщений на электронную почту либо на номера мобильных телефонов с просьбой выполнить определенные действия, связанные с передачей конфиденциальной информации	Вишинг – демонстрация жертве заблаговременно записанного голосового сообщения специалиста – представителя известной компании (например, сотрудника банка), с целью получения конфиденциальных сведений

Претекстинг – комплекс действий, проведенный по определенному, заранее подготовленному сценарию (претексту), с целью получения конфиденциальных сведений от жертвы или направленный на совершение ею определенных действий	«Троянский конь» – отправление жертве сообщения или ссылки в виде вредоносной программы с текстом о мнимом выигрыше; целью выступает списание денежных средств с банковской карты либо заражение персонального компьютера жертвы вирусом при переходе по ссылке или скачивании файла

В зависимости от применяемых информационно-телекоммуникационных средств)	Действия с использованием сотовой или мобильной связи
	Действия с использованием сети Интернет
	Действия с использованием ПЭВМ (персонального компьютера)
	Комбинированные действия, сочетающие в себе два и более названных способа

В зависимости от механизма преступного поведения	Действия через сайты объявлений (преступник выступает в роли продавца)
	Действия, направленные на взлом страницы жертвы в социальных сетях («ВКонтакте», «Одноклассники» и т. д.)
	Действия, совершенные с использованием Интернет-сайтов, интернет-магазинов
	Действия, совершенные под предлогом предотвращения транзакций с банковских карт, при использовании IP-телефонии
	Действия, совершенные под вымышленным предлогом помощи родственнику, знакомому
	Действия, совершенные под видом мнимой бесплатной консультации (юридической, социальной), за которую потом выставляется счет, денежные средства списываются автоматически с банковского счета жертвы

Типичные следы преступлений. Механизм следообразования при совершении преступлений в сфере компьютерной информации. В широком смысле следы – это любые изменения, связанные с событием преступления, отражающие его сущность и специфику. Каждый след несет часть информации, а совокупность следов – всю информацию о преступлении и лицах, его совершивших. В качестве

информации рассматриваются сведения (сообщения, данные) об окружающем мире и протекающих в нем процессах, воспринимаемых человеком и специальными устройствами.

Классификация следов в зависимости от условия формирования		
Статические (точечные) и динамические (линейные)	Локального и периферического воздействия	Объемные и поверхностные

Понятие следов в сфере компьютерной информации в узком смысле

Следы-предметы портативные, многофункциональные или микропроцессорные электронные устройства: персональные компьютеры, ноутбуки, смартфоны, планшеты и другие гаджеты; устройства вывода информации; оборудование компьютерных и беспроводных сетей; детали электронных устройств; документы, рукописные и машинописные записи конфиденциальных сведений; данные банковских карт потенциальных жертв; сим-карты, используемые злоумышленниками, и сим-карты жертв; банковские карты, используемые злоумышленниками, и банковские карты жертв и т. д.

Следы-отображения в виде следов человека, которые остаются на следах-предметах:

следы папиллярных линий рук и ног; следы зубов; следы частей тела; следы одежды; вещественные следы биологического происхождения: следы слюны, крови, волос, пота, запаха и прочих выделений человеческого организма (перхоть, подногтевое содержимое).

Механизм следообразования – это процесс взаимодействия двух и более материальных объектов, конечная цель которого состоит в возникновении следа. Цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде в процессе ее возникновения, обработки, хранения и передачи. Среди следов выделяют идеальные и материальные. Под идеальными следами преступления понимается криминалистически значимая уголовно-релевантная информация, воспринятая и запечатленная человеком в виде мысленных (памятных) образов, которая может быть воспроизведена им в вербальной форме либо извлечена из его памяти средствами, допустимыми для использования в уголовном судопроизводстве.

Идеальные следы возникают в памяти потерпевшего, подозреваемого (обвиняемого), свидетеля, эксперта, специалиста и др.

Материальные следы	Программы для создания сайтов (интернет-магазинов), приложения социальных сетей и сервисов электронной почты, программы, осуществляющие удаленное администрирование
	Анкетные данные пользователя (злоумышленника), указанные в названных программах и приложениях при регистрации
	Текстовые клише, содержащие обращения от имени государственных учреждений, банковских организаций, администраторов социальных сетей
	Черновики электронных писем, содержащих форму для предоставления жертвой конфиденциальной информации либо ссылку для перехода на фишинговый сайт
	Входящие и исходящие электронные сообщения в сети Интернет, а также вся информация, их характеризующая
	Электронные базы персональных и банковских данных жертв
	Информация о веб-браузере компьютера или сотового телефона преступника, содержащем ссылки, истории посещения веб-сайтов, свидетельствующие о способности злоумышленника осуществлять рассылки, сбор и анализ конфиденциальных сведений жертвы
	Электронно-цифровые данные от провайдера сети Интернет (информация об IP-адресах злоумышленников, сведения о доменном имени, сведения о регистрации домена при создании фишингового интернет-сайта и др.)
	Образцы шпионских или вредоносных программ, инструкции по их использованию и внедрению в персональный компьютер или сотовый телефон для кражи конфиденциальных данных жертвы или электронных денежных средств

Криминологическая характеристика лиц, совершающих преступления с использованием компьютерной информации. Лица, совершающие преступления в сфере компьютерной информации, представляют собой специфическую разновидность преступников, обладающих, с одной стороны, общими признаками правонарушителей, с другой – особыми чертами, присущими данной криминальной категории.

В соответствии с общими признаками личность преступника – это совокупность социально приобретенных, относительно устойчивых негативных качеств индивида, обуславливающих его преступное поведение.

Наряду с указанными качествами лицо, совершающее преступления в сфере компьютерной информации, обладает специальными знаниями и навыками, обеспечивающими возможность осуществлять деятельность, направленную на преодоление защитных меха-

низмов на пути к получению информации и незаконному ее использованию. В то же время лицо, совершающее компьютерное преступление, обладает специальными, глубокими по уровню знаниями, прочными навыками, позволяющими ему искать пути вскрытия ограниченной или конфиденциальной информации, раскрывая секреты ее защиты.

В соответствии с представленными признаками в криминологии выделяются различные группы преступников в сфере компьютерной информации.

«Хакер (кракер)»	Наиболее многочисленная группа. Изначально термин использовался для описания талантливого законопослушного программиста-профессионала, способного детально изучить операционные системы, особенности языков программирования и тонкости прикладных пакетов. В криминальном понимании навыки могут использоваться и для совершения преступлений – получения несанкционированного доступа к чужой информации по различным мотивам – от озорства и самоутверждения до промышленного шпионажа. В любом случае это действия, за которые уголовным законом предусмотрено наказание
«Фрикер»	лицо, специализирующихся на использовании телефонных систем с целью уклонения от оплаты телекоммуникационных услуг
«Кардер»	индивид, оплачивающий свои расходы с чужих кредитных карточек
«Киберворон»	преступник, использующий компьютерные программные продукты, перехватывающий различные пароли, а также коды телефонного вызова и номера телефонных компаний, имеющих выход к компьютерным сетям общего использования, например Интернет
«Коллекционер»	злоумышленник, который специализируется на несанкционированном проникновении в компьютерные системы финансовых, банковских расчетов. Обычно они используют компьютерные технологии для получения номеров кредитных карточек и другой ценной информации с целью наживы. Нередко полученную информацию они продают другим лицам
«Компьютерный пират»	персонаж, специализирующийся на незаконном взломе систем защиты лицензионных компьютерных программных продуктов, распространяемых потом за деньги по ценам, которые значительно ниже цен законных изготовителей

Соотношение преступников в сфере компьютерной информации по признаку пола 5:1 в пользу мужчин. Как правило, компьютерные преступники имеют высшее или неоконченное высшее техническое образование (54%), а также другое высшее либо неоконченное высшее образование (19%). Около 52% правонарушителей имели специальную подготовку в области автоматизированной компьютерной обработки информации, 97% выявленных преступников были сотрудниками государственных учреждений и организаций, которые использовали компьютерные системы и информационные технологии в своей повседневной деятельности. При этом 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

Возрастной диапазон компьютерных правонарушителей колеблется в пределах от 14 до 45 лет. 54% преступников – это лица в возрасте от 18 до 25 лет; 13% – от 26 до 40 лет.

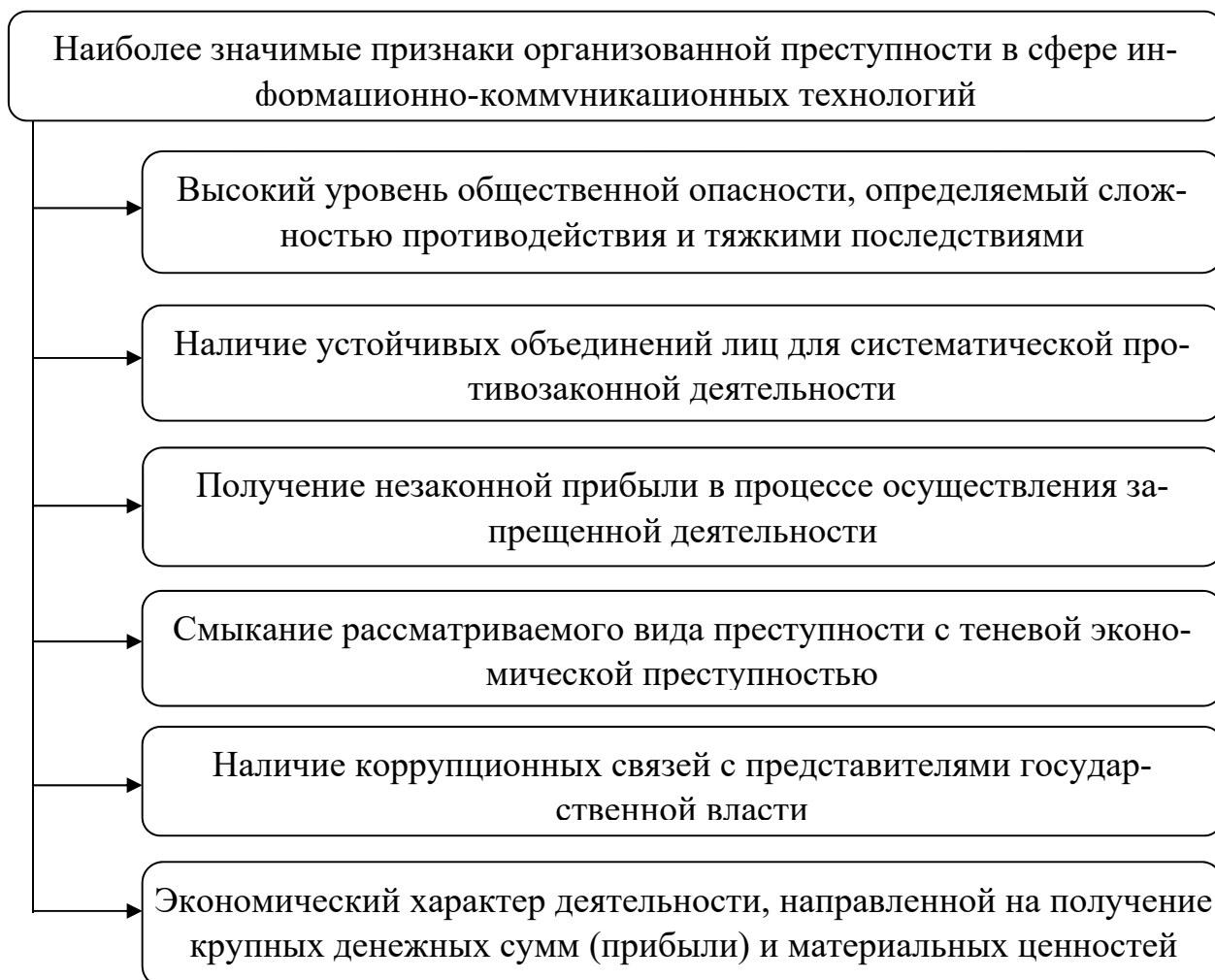
С точки зрения морально-психологических характеристик рассматриваемый преступник, как правило, творческая личность, способная идти на вызов, риск. Криминологические исследования позволили разделить таких правонарушителей на три мотивационных категории, существенно отличающихся друг от друга степенью общественной опасности.

Наиболее многочисленной, но наименее опасной категорией являются так называемые *хакеры-дилетанты*. На их долю приходится до 80% всех компьютерных атак. Но этих людей интересует не некая цель, а сам процесс атаки. Они испытывают удовольствие от преодоления систем защиты. Чаще всего их действия удастся легко пресечь, поскольку хакеры-любители предпочитают не рисковать и не вступать в конфликт с законом.

С повышением уровня профессионализма, связанного с фактическим получением высшего технического образования, дилетанты трансформируются во вторую мотивационную категорию. Они приобретают более глубокие, систематизированные знания в области компьютерных технологий и являются *специалистами*. Психологически люди данной группы более уравновешенны, имеют отчетливо сформированную систему взглядов и ценностей, однако высокий уровень амбициозности им все же пока не присущ.

Основной сферой преступной деятельности «специалистов» являются сетевой взлом, действия в операциях по получению конфиденциальной информации, обладающей мощными системами защиты данных, промышленный и интеллектуальный шпионаж.

Характерные особенности преступных групп, осуществляющих преступную деятельность в сфере компьютерной информации



Примерный план занятия

1. Понятие и состав криминалистической характеристики преступлений, совершаемых с использованием компьютерной информации.

2. Криминалистический анализ Интернета как особой информационно-коммуникационной сети: субъекты, объекты, техническое и правовое регулирование.

3. Наиболее распространенные способы совершения преступлений с использованием сети Интернет. Типичные следы преступлений. Механизм следообразования при совершении преступлений в сфере компьютерной информации.

4. Криминологическая характеристика лиц, совершающих преступления с использованием компьютерной информации. Характерные особенности преступных групп, осуществляющих преступную деятельность в данной сфере.

Вопросы для самоконтроля по теме

1. Каковы отличительные черты личности преступников в сфере компьютерной информации?
2. Какова наиболее многочисленная группа преступников в сфере компьютерной информации?
3. В чем заключаются специфические черты личности компьютерного преступника по классификации «компьютерный пират»?
4. Каково значение специальной подготовки в деятельности компьютерных преступников?
5. Чем обусловлено смыкание организованной преступности в сфере ИКТ с теневой экономической преступностью?

Тема 1.4. Современное состояние борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий

Преступность в сфере ИКТ представляет собой совокупность преступлений, совершаемых с использованием методов, производственных процессов и программно-технических средств, которые интегрированы с целью сбора, обработки, хранения, распространения, отображения и последующего использования информации в интересах ее пользователей.

Важным показателем криминологической значимости оценки преступности в сфере ИКТ выступает появление в ежегодной статистической отчетности МВД России нового раздела «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий»¹. Структура этого нового вида преступности до настоящего времени подвергается постоянной коррекции, что видно даже по названию раздела, который с 2020 г. носит название «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации».

К настоящему моменту правовая статистика располагает тремя законченными отчетными периодами, по которым имеются исчерпывающие за определенный промежуток времени данные, которые можно подвергнуть сравнительному анализу. Между тем ознакомление с краткой характеристикой состояния преступности в Российской Федерации за январь – декабрь 2019 г., предваряющей изложение основного массива статистических сведений в указанной отчетности, позволяет выявить сравнение с предыдущим отчетным периодом – 2018 г. В частности, в п. 9 упомянутой характеристики указывается: «В январе–декабре 2019 г. зарегистрировано 294,4 тыс. преступлений, совершенных с использованием ИКТ, или на 68,5% больше, чем за аналогичный период прошлого года». Однако в предыдущей статистической отчетности таких сведений нет. Предполагается, что информация почерпнута из внутренней формы отчетности 1-ВТ.

В 2021 г. при изложении статистических показателей рассматриваемого вида преступности в отчетности делается ссылка на межведомственный нормативный источник, регламентирующий составление статистической отчетности: «Показатели сформированы в соот-

¹ URL: <https://мвд.рф/folder/101762/> (дата обращения: 05.05.2022).

ветствии с Перечнем № 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 29 декабря 2021 г. № 790/11/1»¹.

Результаты статистического учета преступлений, совершаемых с использованием ИКТ в официальной статистической отчетности

В январе–декабре 2019 г. зарегистрировано 294,4 тыс. преступлений, совершенных с использованием ИКТ или на 68,5% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8% в январе–декабре 2018 г. до 14,5%. Практически все такие преступления (98,4%) выявляются органами внутренних дел.

Почти половина таких преступлений (48,5%) относится к категориям тяжких и особо тяжких: 142,7 тыс. (+149,0%); половина (53,3%) совершается с использованием Интернета: 157,0 тыс. (+45,4%), более трети (39,5%) – средств мобильной связи: 116,2 тыс. (+89,5%).

Четыре таких преступления (80,0%) из пяти совершаются путем кражи или мошенничества: 235,5 тыс. (+83,2%), каждое двенадцатое (8,4%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 24,7 тыс. (+31,2%).

В январе–декабре 2020 г. зарегистрировано 510,4 тыс. преступлений, совершенных с использованием ИКТ или на 73,4% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5% в январе–декабре 2019 г. до 25,0%. Практически все такие преступления (98,6%) выявляются ОВД.

Больше половины таких преступлений (52,4%) относится к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5%); больше половины (58,8%) совершается с использованием Интернета: 300,3 тыс. (+91,3%), почти половина (42,9%) – средств мобильной связи: 218,7 тыс. (+88,3%).

Четыре таких преступления (80,4%) из пяти совершаются путем кражи или мошенничества: 410,5 тыс. (+74,3%), почти каждое одиннадцатое (9,2%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 47,1 тыс. (+90,7%).

¹ URL: (дата обращения: 05.05.2022).

В январе–декабре 2021 г. зарегистрировано 517,7 тыс. преступлений, совершенных с ИКТ или в сфере компьютерной информации, что на 1,4% больше, чем за аналогичный период прошлого года.

В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,0% в январе–декабре 2020 г. до 25,8%. Практически все такие преступления (98,8%) выявляются ОВД.

Больше половины таких преступлений (55,7%) относится к категориям тяжких и особо тяжких (288,3 тыс.; +7,7%), более двух третей (67,9%) совершается с использованием сети Интернет (351,5 тыс.; +17,0%), почти половина (42,0%) – средств мобильной связи (217,6 тыс.; -0,5%).

Более чем три четверти таких преступлений (78,4%) совершается путем кражи или мошенничества: 406,0 тыс. (-1,1%), почти каждое десятое (9,9%) – с целью незаконного производства, сбыта или пересылки наркотических средств: 51,4 тыс. (+9,3%).

Рейтинг регионов по темпам прироста преступлений, совершаемых с использованием ИКТ за 2021 г.

Регионы с наиболее высоким темпом роста	Регионы с наименьшим темпом роста
Чеченская Республика 135,0%	Еврейская АО -24,8%
Тульская область 64,4%	Тверская область -23,9%
Республика Адыгея 45,8%	Новосибирская область -19,4%
Московская область 37,4%	Рязанская область -18,0%
Республика Дагестан 30,0%	Республика Алтай -17,9%
Ярославская область 26,0%	Архангельская область -17,6%
Республика Саха (Якутия) 25,8%	Ямало-Ненецкий АО -17,6%
Краснодарский край 17,3%	Ивановская область -17,1%
Челябинская область 17,2%	КЧР -16,6%
КБР 17,1%	Псковская область -13,8%

Рейтинг регионов по удельному весу преступлений, совершаемых с использованием ИКТ за 2021 г.

Регионы с высоким удельным весом	Регионы с низким удельным весом
ХМАО-ЮГРА 39,3%	Республика Дагестан 8,1%
г. Москва 39,3%	Чеченская Республика 8,8%
Чувашская Республика 37,2 %	Республика Тыва 10,6%
Ямало-Ненецкий АО 35,8 %	Республика Ингушетия 11,7%
г. Санкт-Петербург 35,0%	Республика Алтай 15,3%
Республика Татарстан 33,8%	Архангельская область 15,5%

Мурманская область 32,6%	Республика Бурятия 16,3%
Кировская область 31,3%	Еврейская АО 16,6%
Республика Марий Эл 31,3%	Московская область 17,1%
Республика Коми 31,1%	РСО-Алания 17,2%

Рейтинг регионов по раскрываемости преступлений, совершаемых с использованием ИКТ за 2021 г.

Регионы с наибольшей раскрываемостью	Регионы с наименьшей раскрываемостью
Псковская область 49,5%	Ленинградская область 11,7%
Чукотский АО 45,0%	Амурская область 13,8%
Республика Дагестан 38,9%	Смоленская область 14,4%
Республика Алтай 36,5%	Чеченская Республика 15,5%
Московская область 35,6%	Тульская область 15,9%
КЧР 35,3%	Приморский край 17,1%
Челябинская область 34,7%	Новосибирская область 17,3%
Республика Ингушетия 33,5%	Тверская область 17,4%
Рязанская область 33,1%	Алтайский край 17,6%
Республика Мордовия 32,5%	г. Москва 17,6%

Структура преступности, связанной с использованием ИКТ в 2021 г.

Мошенничество	48%
Кража	30%
Незаконный оборот наркотиков	10%
Преступления в сфере компьютерной информации	1%
Распространение материалов порнографического характера	10%
Иные преступления	1%

Причинный комплекс преступности в сфере ИКТ

Социально-экономические	Кризисные явления в экономике; низкий уровень жизни большинства населения; резкая дифференциация общества по материальному признаку; высокий уровень безработицы; неудовлетворительный уровень социальной защищенности наиболее уязвимых слоев населения

Правовые	Недостатки действующего информационного законодательства, страдающего отсутствием системности и планомерности развития и законодательного регулирования; несоответствие уголовного законодательства существующим общественно опасным явлениям в информационной сфере; правовая неграмотность и правовой нигилизм значительной части населения; чрезвычайно широкая распространенность преступлений в сфере компьютерных технологий и высоколатентный характер данных преступлений, обусловленный самыми разными причинами; неустоявшаяся судебная-следственная и прокурорская практика, отсутствие научно обоснованных методических рекомендаций по раскрытию, расследованию и квалификации такого рода преступлений; отсутствие какой-либо достоверной статистики преступности в сфере компьютерных технологий, ее состояния, структуры и динамики
Технические	Повсеместность использования соответствующей инфраструктуры, сетей, программ, оборудования, а также растущее во всем мире и в России количество пользователей программно-технических средств; доступность компьютерных технологий; возрастающая зависимость современных технологий от компьютерных систем и средств телесвязи; высокий уровень анонимности пользователей ИКТ; чрезвычайно высокая скорость совершения преступного воздействия на среду влияния и практическое отсутствие материальных следов; высочайшая степень свободы, ввиду отсутствия эффективных предохранителей на каналах общения в киберпространстве
Организационно-управленческие	Несоответствие системы международных стандартов в области компьютерной техники, связи и информационной безопасности требованиям времени; отсутствие должного международно-правового сотрудничества в сфере противодействия преступности в области компьютерных технологий; отсутствие комплексных государственных мер, направленных на противодействие преступлениям в указанной сфере; несовершенство социальных, юридических и политических структур, уровень развития которых значительно отстает от уровня развития компьютерных и телекоммуникационных технологий
Политические	Участие в ряде стран специальных государственных структур в незаконном проникновении в компьютерные сети в геополитических и военно-стратегических целях этих государств

Примерный план занятия

1. Структура и динамика преступлений, совершаемых в сфере ИКТ.
2. Показатели уголовно-правовой статистики преступлений, совершаемым в сфере ИКТ.
3. Виды и формы преступности в сфере ИКТ.
4. Детерминанты преступности в сфере ИКТ в России.

Вопросы для самоконтроля по теме

1. Назовите специфические черты преступности в сфере ИКТ.
2. В чем заключается высокая криминологическая значимость самостоятельного изучения преступности в сфере ИКТ?
3. Каковы особенности современной статистической отчетности МВД России в сфере оценки компьютерной преступности?
4. Охарактеризуйте результаты статистического учета преступлений в сфере ИКТ за последние три года.
5. Классифицируйте причины и условия совершения преступлений в сфере ИКТ.

Тема 1.5. Организация профилактической работы по предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий

Одним из последствий внедрения ИКТ в основные процессы жизнедеятельности является значительный рост преступлений, совершаемых с их применением.

Нормативные акты, являющиеся правовой основой предупреждения преступлений, совершаемых с использованием ИКТ	
ФЗ «Об информации»	В тексте закона содержатся основные понятия по вопросам, связанным с ИКТ
ФЗ от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Расширяет список понятий, применяемых в данной области, например: компьютерная атака, компьютерный инцидент, автоматизированная система управления
УПРФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»	Устанавливает порядок обеспечения безопасности развернутых и создаваемых на территории России информационных систем (как одно из основных направлений в государственной деятельности), а также защиту информационных ресурсов от несанкционированного доступа
УПРФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»	Содержит положения по обеспечению комплексной защиты информационной инфраструктуры РФ, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, как одной из основных задач, поставленных перед государственными органами

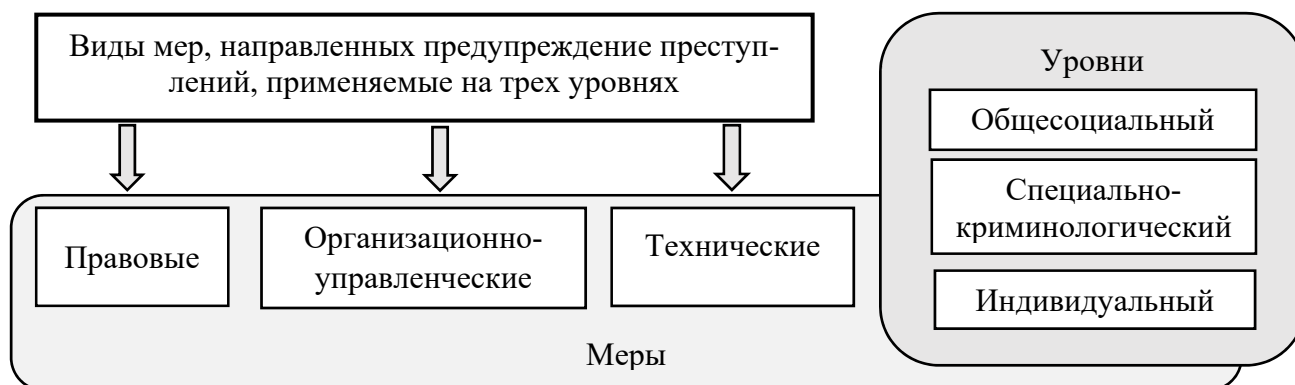
УПРФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» национальная программа «Цифровая экономика Российской Федерации»	Национальные цели и задачи в данной области заключаются в развитии цифровой экономики, создании устойчивой и безопасной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств, использовании преимущественно отечественного ПО государственными органами, органами местного самоуправления и организациями

На данный момент понятие предупреждения преступности в части совершения преступлений с использованием ИКТ не сформировано. Наиболее удобным определением может служить следующее.

Предупреждение (превенция) преступности – это любая деятельность государственных органов или отдельных лиц, которые намереваются устранить преступление до его совершения или до того, как будут совершены какие-либо дополнительные действия.

Профилактика и предупреждение преступлений, совершаемых с использованием ИКТ, направлены на выработку мер и создание условий, при которых осуществление любой деятельности, связанное с использованием ИКТ, сетей и компьютерной информации в целом, будет происходить при минимальном уровне неправомерных действий.

Преступления, совершаемые с использованием ИКТ, обладают определенной спецификой, благодаря которой представляется возможным выделить группы мер, направленных на предупреждение преступности.

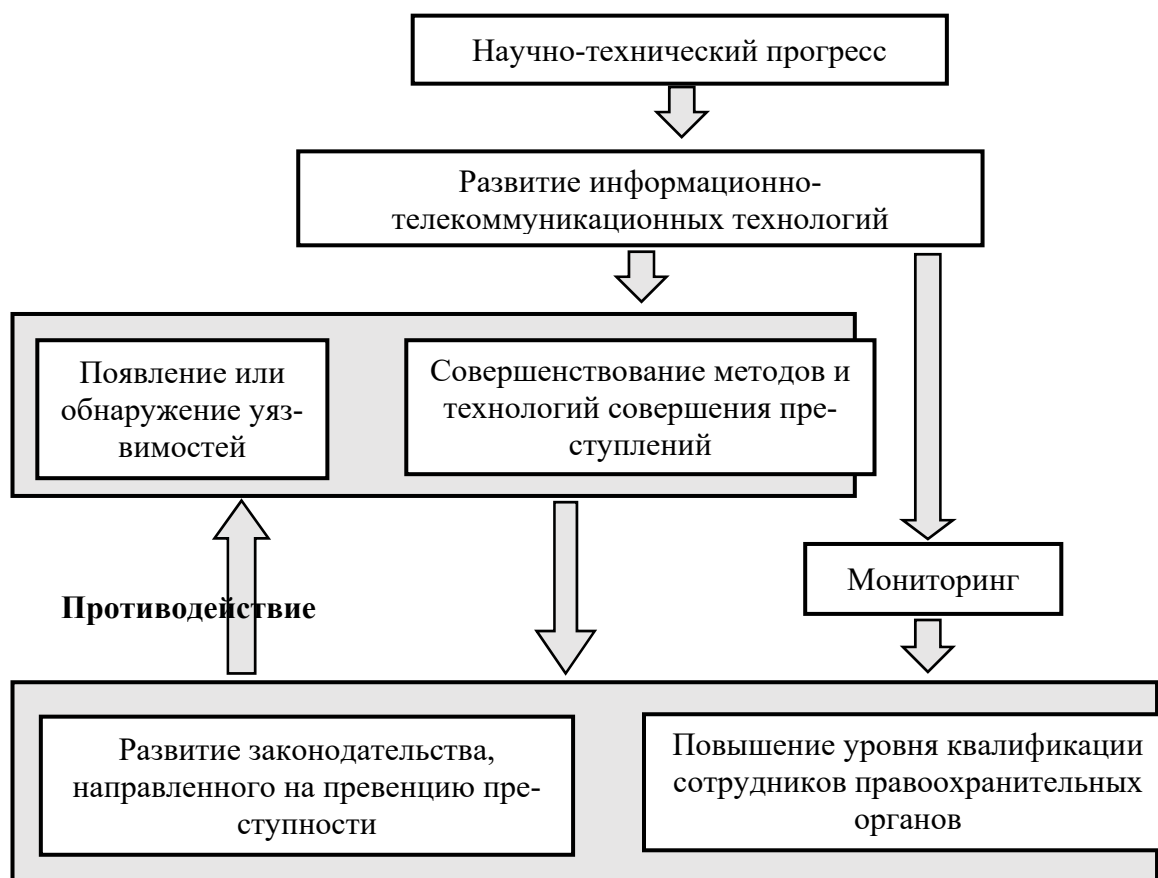


Предупреждение преступности – сложная система, которая включает в себя отдельные элементы деятельности, направленные на осуществление воздействия на причины и условия, способствующие совершению преступлений, а также на совершивших их лиц. Предупреждение преступлений имеет многоуровневый характер, что обусловлено наличием как долговременных и достаточно масштабных мер, таких как принятие Доктрины информационной безопасности РФ, так и не менее важных мер индивидуальной работы по предотвращению преступлений в сфере ИКТ.

Общесоциальный уровень предупреждения преступлений направлен на решение комплексных социальных проблем, в результате чего повышается эффективность профилактики преступности. Общесоциальный уровень не воздействует непосредственно на криминальные процессы в обществе, решение социальных проблем косвенно влияет на причины и условия совершения преступлений как в целом, так и в данной сфере общественной жизни.

Общесоциальные меры предупреждения преступлений в сфере ИКТ условно разделяются на несколько основных направлений	
<i>Общезкономическое</i>	Воздействие – это создание условий для экономического роста в целях повышения конкурентоспособности с помощью информационных технологий воздействующих на развитие цифровой экономики, ликвидацию бюрократических барьеров, повышение производительности труда и снижение уровня коррупции
<i>Социальное</i>	Направлено на противодействие социальному и имущественному расслоению общества, развитие устойчивой социальной политики и своевременное разрешение социальных вопросов. Например, достойная оплата труда, реализация качественных товаров, система личной безопасности граждан
<i>Научно-техническое</i>	Направлено на осуществление государственной поддержки системы научных исследований фундаментального характера как части национальной безопасности государства. Осуществляется посредством создания научно-исследовательских и образовательных учреждений, подготовки специалистов и как итог – разработки новых образцов наукоемкой продукции
<i>Общекультурное</i>	Необходимо для укрепления духовного единства граждан России, повышения имиджа российской культуры за рубежом и роли культуры в жизни каждого россиянина посредством патриотического воспитания

Законодательное	Выражается в повышении качества принимаемых нормативных актов. Мониторинг является частью системы реагирования государства на возникновение угроз обществу и государству и направлен на осуществление координации в области развития законодательства и применения правовых норм, их соответствие международным стандартам борьбы с преступностью, международным соглашениям, а также создание процедуры криминологической экспертизы законопроектов



Уровень специально-криминологического предупреждения направлен на причины и условия совершения преступлений, осуществляемых с использованием ИКТ. Основные направления деятельности субъектов превенции преступности включают:			
Повышение эффективности научного обеспечения деятельности по противодействию преступности в сфере ИКТ	Совершенствование системы правоприменения, в том числе разработка новых форм и методов борьбы с преступлениями в сфере ИКТ	Принятие организационно-управленческих мер предупреждения преступлений, совершаемых с использованием высоких технологий	Комплекс целенаправленных мероприятий по устранению причин и условий, способствующих совершению компьютерных преступлений

Индивидуальный (виктимологический) уровень противодействия преступлениям в части ИКТ.

В криминологии как науке поведение жертвы является одним из составных элементов механизма преступления. Специфической особенностью преступлений, совершаемых с использованием ИКТ, является воздействие на жертву, имеющую низкий уровень грамотности в данной области. Для повышения уровня эффективности предупреждения преступности в данной сфере необходимо применять меры виктимологической профилактики, которая должна быть направлена на потенциальных жертв преступлений.

Система субъектов профилактики преступности в сфере ИКТ. К субъектам виктимологической профилактики преступлений, связанных с ИКТ, относится государство в лице правоохранительных органов, а также негосударственные структуры, т. е. различные общественные объединения. Профилактика данного вида преступлений охватывает различные формы виктимного поведения: незнание элементарных мер защиты, пользовательскую небрежность и в целом легкомысленность поведения, излишнее любопытство, возрастные и интеллектуальные особенности и другое. Регулирование виктимологической защиты осуществляется не только через правовые нормы, но и посредством морали. Профилактика преступности ориентируется на социальное предупреждение в целях снижения количества совершения преступлений в области ИКТ.

Важную роль в предупреждении преступлений в сфере ИКТ играют государственные и общественные институты.

Для обеспечения эффективного противодействия совершению преступлений в сфере ИКТ и для стабильной работы объектов критической информационной инфраструктуры существует система **ГосСОПКА** (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации). Данная система создана в прямом взаимодействии государственных органов и коммерческих структур. Цель данной организации – осуществление государственного контроля за безопасностью критической информационной инфраструктуры РФ и оценки степени их защищенности от компьютерных атак.

Обеспечение безопасности критической инфраструктуры в сфере информационных технологий зависит не только от государственного контроля, но и от того, как субъекты критической инфраструктуры выполняют требования по созданию систем безопасности и обеспечивают их функционирование. Такие требования внесены в перечень в соответствии с приказом Федеральной службы по техническому и экспортному контролю.

В процессе предупреждения преступности правоохранительные органы традиционно занимают центральное место. Одной из наиболее важных задач ОВД становится просвещение населения в области ИКТ, направленное на предотвращение киберпреступности. Необходимо не ограничиваться простым информированием, т. е. доведением до населения конкретных мошеннических схем и способов, используемых преступниками, так как данные схемы регулярно видоизменяются, а за счет большой территории Российской Федерации могут появляться так называемые «очаговые» схемы, которые имеют ограниченное распространение в отдельных субъектах. Обычная схема деятельности ОВД по информированию населения является не только малоэффективной, но и в определенных случаях может иметь отрицательный эффект. Необходимо учитывать, что в области ИКТ существенный криминогенный фактор – это небрежность пользователей при защите персональной информации. Для пожилых людей, являющихся наиболее виктимной группой в силу их легкомысленного пользования личными данными, такая информация окажется бесполезной, а правонарушители смогут взять удачные схемы «коллег» на вооружение.

Полномочия ОВД по профилактике преступлений, совершаемых с использованием ИКТ, являются достаточно ограниченными.

Основным направлением деятельности в данной области является доведение до граждан базовых правил безопасного использования информационных технологий, к которым относится опасность совершения следующих действий	
Неумелое пользование сетью Интернет. Осуществление различных банковских операций на сайте без проверки правильности введенного адреса сайта	Загрузка программ из непроверенных источников, переход по рекламным ссылкам, в которых могут содержаться вредоносные программы или которые ведут на мошеннические сайты, просмотр и открытие электронной почты от неизвестных адресатов; регистрация на различных сайтах или интернет-ресурсах с одинаковыми или простыми паролями
Общение в социальных сетях с неverified личностями, размещение в них личной информации, например, о планируемом отпуске	Их целью может являться совершение правонарушений в отношении пользователя
Приобретение SIM-карт не в специализированных магазинах-салонах связи, а у случайных людей	Влечет оставление паспортных данных каким-либо сомнительным организациям

Передача денежных средств	Например, лицам, которые якобы предлагают услуги, связанные с решением проблем у родственников или знакомых, которые якобы «попали в беду»
Совершение правонарушений в отношении пользователя, в том числе кража денежных средств со счетов пользователя	Передача личных данных с кредитных или дебетовых карт, сообщение личного пароля и кодовых слов, запрашиваемых по телефону или через социальные сети от лица банковских, кредитных или иных организаций, друзей и знакомых под различными предложениями. Незнание порядка действий, связанных с блокированием кредитной или дебетовой карты при получении сообщения о снятии или переводе денежных средств третьим лицам
Оставление записанных личных данных, в том числе паролей в публичных местах	Стикеры с логином и паролем, приклеенные к монитору на рабочем месте

Примерный план занятия

1. Правовая основа, понятие, направления профилактики в сфере ИКТ.
2. Общее, специальное и индивидуальное предупреждение преступности в сфере ИКТ.
3. Система субъектов профилактики преступности в сфере ИКТ.
4. Государственные и общественные институты как субъекты предупреждения преступности в сфере ИКТ.
5. Место органов внутренних дел в системе профилактической деятельности.
6. Полномочия органов внутренних дел по профилактике преступлений, совершаемых с использованием ИКТ.

Вопросы для самоконтроля по теме

1. Какие термины используются в ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»?
2. Какие цели и задачи закреплены в Доктрине информационной безопасности Российской Федерации?
3. Какие меры сотрудники органов внутренних дел имеют право применять в соответствии с приказом МВД России от 17 января 2006 г. № 19 «О деятельности органов внутренних дел по предупреждению преступлений»?

Тема 1.6. Международный опыт противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Центральной проблемой международного сотрудничества по борьбе с преступлениями в сфере информационно-коммуникационных технологий является существенное отличие нормативного регулирования борьбы с компьютерными преступлениями в отдельных государствах.

Особенности современного состояния международного сотрудничества в борьбе с киберпреступлениями:

- ограничение сотрудничества в рамках региональных организаций и межгосударственных объединений, создающих свои способы взаимодействия;
- отсутствие общепринятых определений рассматриваемого вида преступности и его признаков;
- отсутствие систематизированного законодательства, охватывающего все стороны борьбы с компьютерными преступлениями;
- существенное отставание действующих законов от стремительно развивающихся условий жизни общества и общественных отношений в информационной сфере;
- наличие множества противоречий в осуществлении международного сотрудничества по причине нарушения суверенитета отдельных государств.

Перспективные направления совершенствования международного сотрудничества в борьбе с компьютерными преступлениями:

- формирование единого подхода к пониманию существующих в данной сфере проблем и путей борьбы с преступлениями в сфере информационных технологий;
- создание специализированных межгосударственных ведомств, объединяющих специалистов в различных сферах;
- вовлечение в процесс противодействия компьютерным преступлениям представителей негосударственных формирований, объединений и отдельных граждан;
- разработка международных процессуальных механизмов расследования выявленных преступлений, исследования и предоставления электронных доказательств;
- формирование глобальных механизмов противодействия преступности в сфере информационных технологий, укрупнение существующих региональных объединений.

Международные организации, осуществляющие противодействие преступлениям в сфере ИКТ и сотрудничества по линии Интерпола:

- Европейский центр борьбы с киберпреступностью;
- Европейский центр по борьбе с финансовыми и экономическими преступлениями (EFECC);
- Международный альянс J5 по борьбе с серьезными международными преступлениями;
- Консультативная группа Европола SOCTA по подготовке и одобрению методологии и определению требований к сбору оперативных данных, их анализу, определению основных криминологических рисков и угроз, составлению отчетов по итогам исследований, а также подготовке предложений по приоритетным направлениям.

Перспективные направления деятельности Интерпола по борьбе с преступлениями в сфере информационных технологий:

- киберразведка и анализ;
- оперативная и следственная поддержка;
- цифровая криминалистика;
- национальные кибер-обзоры;
- технологические инновации и научные исследования.

Зарубежный опыт противодействия преступлениям в сфере ИКТ

Первый специальный закон, касающийся информационных преступлений, были издан в Швеции в 1973 г. Специальные нормы или даже разделы о компьютерных преступлениях содержат все новые уголовные кодексы, принятые в мире начиная с 1992 г., в том числе УК всех стран на территории бывшего СССР.

Государства, в настоящий момент располагающие наиболее эффективными стратегиями кибербезопасности	
Государства – члены Евросоюза	Иные государства
Великобритания, Германия, Голландия, Литва, Люксембург, Словакия, Финляндия, Франция, Чехия, Швеция, Эстония	США, Канада, Япония, Индия, Австралии, Новая Зеландия, Колумбия

Борьба с преступлениями в сфере информационных технологий рассматривается в большинстве указанных стран не только в русле уголовной политики, но и в рамках стратегии обеспечения национальной безопасности. В полной мере это относится к Российской Федерации.

Основные подходы к криминализации деяний в сфере информационных технологий	
Первый подход Преступления, связанные с использованием компьютерной техники и информации, выделяются в специальную главу исходя из того, что главным объектом посягательства для всех них является информационная безопасность (страны СНГ, кроме Казахстана, Узбекистана, Андорра, Литва, Монголия, Польша, Румыния, Сербия, Черногория)	Второй подход Учитывается, что у любого из компьютерных преступлений свой конкретный объект посягательства (собственность, права личности, общественная безопасность и т. д.), поэтому составы рассматриваемых деяний рассредоточены по соответствующим разделам Особенной части уголовного закона (Австрия, Германия, Испания, Эстония, Япония)
Основные проблемы использования указанных подходов в правоприменительной практике	
Полностью выделить компьютерные преступления из общей массы других деяний просто невозможно, так как между ними отсутствуют четкие границы	Распределение данных составов по различным разделам и главам Особенной части уголовного закона существенно затрудняет составление статистической отчетности
Имеются и промежуточные варианты построения уголовно-правовых норм, например: во Франции, Хорватии, Швейцарии и Эстонии специальные составы компьютерных преступлений отнесены к преступным деяниям против имущества	
В Российской Федерации уголовное законодательство содержит отдельную главу «Преступления в сфере компьютерной информации», по которой имеется отдельная статистическая отчетность. В официальном статистическом сборнике появился раздел «Сведения о преступлениях, совершенных с использованием ИКТ или в сфере компьютерной информации». Причина: по мере информатизации современного общества использование ИКТ все чаще становится способом совершения преступлений, нередко существенно повышая их общественную опасность. Это, в свою очередь, требует пересмотра всех элементов системы предупреждения преступности в России	

Основные составы компьютерных преступлений в уголовном законодательстве зарубежных стран

Наименование преступления	В каких государствах встречается
Несанкционированный доступ в компьютерные сети	СНГ, Австралия, Бельгия, Боливия, Великобритания, Германия, Дания, Ирландия, Канада, КНР, Колумбия, Латвия, Мексика, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сербия, Словения, США, Франция, Хорватия, Швейцария, Эстония
Создание и распространение компьютерных вирусов	СНГ и стран Балтии, Бельгия, Вьетнам, Гватемала, Индия, Италия, КНР, Монголия, Нидерланды, Сербия, США, Швейцария
Компьютерный саботаж	Армения, Беларусь, Германия, Кыргызстан, Нидерланды, Парагвай, Польша, Португалия, Сербия, Таджикистан, Эстония
Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной информации и компьютерной системе или их сети	Армения, Беларусь, Великобритания, Италия, Канада, КНР, Монголия, США, Таджикистан, Украина, Хорватия
Нарушение правил эксплуатации компьютерной системы или сети	Азербайджан, Армения, Беларусь, Вьетнам, Грузия, Кыргызстан, Латвия, Молдова, Таджикистан, Украина
Хищение путем использования компьютерной техники	Армения, Беларусь, Боливия
Компьютерное мошенничество	Австрия, Сербия, Хорватия, Черногория, Эстония, Япония

Наряду с вышеперечисленными в отдельных странах в последние годы появляются и другие составы преступлений, которые можно отнести к компьютерным: кибертерроризм (Грузия, США), распространение спама (США, Украина), компьютерный подлог (Бельгия, Хорватия), использование компьютерных данных и технологий в корыстных целях извлечения прибыли путем создания финансовых и других пирамид (Канада).

Примерный план занятия

1. Международное сотрудничество правоохранительных органов по противодействию преступлениям, совершаемым в сфере ИКТ.
2. Международные организации, осуществляющие противодействие преступлениям в сфере ИКТ и сотрудничество по линии Интерпола.
3. Зарубежный опыт противодействия преступлениям в сфере ИКТ.

Вопросы для самоконтроля по теме

1. Перечислите основные положения, характеризующие современное международное сотрудничество в сфере противодействия киберпреступлениям.
2. Назовите наиболее значимые проблемы, с которыми сталкивается международное сообщество в процессе борьбы с киберпреступностью.
3. Назовите направления совершенствования международного сотрудничества в борьбе с компьютерными преступлениями.
4. Какие международные организации являются субъектами, осуществляющими противодействие преступлениям в сфере ИКТ и сотрудничество по линии Интерпола?

Перечень нормативных правовых актов, основной и дополнительной учебной литературы

Нормативные правовые акты

1. Конституция РФ: принята всенародным голосованием 12.12.1993 с изм., одобренными в ходе общероссийского голосования 01.07.2020. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (с изм. и доп. на 30.12.2021). Доступ из справ.-правовой системы «Гарант».
3. О государственной тайне: закон РФ от 21.07.1993 № 5485-1 // Собр. законодательства РФ. 1997. № 41. Стр. 8220–8235.
4. О внешней разведке: федер. закон от 10.01.1996 № 5-ФЗ // Собр. законодательства РФ. 1996. № 3. Ст. 143.
5. О полиции: федер.закон от 07.02.2011 № 3-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
6. О безопасности: федер. закон от 28.12.2010 № 390-ФЗ. Там же.
7. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон от 26.07.2017 № 187-ФЗ. Там же.
8. О государственной тайне: закон РФ от 21.07.1993 № 5485-1 (последняя ред.). Там же.
9. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ. Там же.
10. Об информации, информационных технологиях и защите информации: федер. закон от 27.07.2006 № 149-ФЗ. Там же.
11. Об организации предоставления государственных и муниципальных услуг: федер. закон от 27.07.2010 № 210-ФЗ // Собр. законодательства РФ. 2010. № 31. Ст. 4176.
12. Об электронной подписи: федер. закон от 06.04.2011 № 63-ФЗ. Там же.
13. О техническом регулировании: федер. закон от 27.12.2002.
14. Об утверждении Доктрины информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646.
15. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: указ Президента РФ от 12.04.2021 № 213. Доступ из справ.-правовой системы «КонсультантПлюс».
16. Вопросы федеральной службы безопасности Российской Федерации: указ Президента РФ от 11.08.2003 № 960 // Собр. законодательства РФ. 2003. № 33. Ст. 3254.
17. Вопросы Министерства обороны Российской Федерации: указ Президента РФ от 16.08.2004 № 1082 // Собр. законодательства РФ. 2004. № 34. Ст. 3538.

18. Вопросы Федеральной службы по техническому и экспортному контролю: указ Президента РФ от 16.08.2004 № 1085 // Собр. законодательства РФ. 2004. № 34. Ст. 3541.

19. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 09.05.2017 № 203.

20. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента РФ от 07.05.2018 № 204.

21. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: указ Президента РФ № 31с от 15.01.2013 // Собр. законодательства РФ. 2013. № 3. Ст. 178.

22. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ Федеральной службы по техническому и экспортному контролю № 235 от 21.12.2017. URL: www.pravo.gov.ru.

23. Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия: приказ ФСБ РФ от 13.11.1999 № 564.

24. Вопросы организации информационно-аналитической работы в управленческой деятельности органов внутренних дел Российской Федерации: приказ МВД России от 26.09.2018 № 623. Доступ из справ.-правовой системы «КонсультантПлюс».

25. Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации: приказ МВД России от 31.12.2013 № 1040. Там же.

26. О деятельности органов внутренних дел по предупреждению преступлений (вместе с Инструкцией о деятельности органов внутренних дел по предупреждению преступлений): приказ МВД России от 17.01.2006 г. № 19.

Основная литература

1. Алескеров В.И., Колокольчикова О.Н. Раскрытие преступлений в сфере телекоммуникаций и компьютерной информации: учеб.-практ. пособие // Труды сотрудников Всероссийского института повышения квалификации сотрудников МВД России. – Домодедово: ВИПК МВД России, 2018. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

2. Апульцин В.А., Гонов Ш.Х., Лебедев В.Н., Петрова В.Ю. Информационные технологии управления и организации защиты информации: курс лекций. М.: Академия управления МВД России. 2021.

3. Баранов В.В. и др. Информационные технологии в управлении и организации защиты: учеб. / под ред. И.В. Горошко. М.: Академия управления МВД России, 2018.

4. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие. / сост. А.В. Аносов. М.: Академия управления МВД России, 2019. Ч. 1. 208 с. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

5. Лебедев В.Н. и др. Защита информации: учеб.: в 2 ч. / под ред. В.И. Кирина. М.: Академия управления МВД России, 2013.

6. Лукашов Н.В., Лебедев В.Н., Макаров В.Ф. Информатизация и информационная безопасность органов внутренних дел: курс лекций. М.: Академия управления МВД России, 2012.

Дополнительная литература

1. Гаврилов М.В., Климов В.А. Информатика и информационные технологии: учеб. 3-е изд., перераб. и доп. М. : Юрайт, 2013. 378 с.

2. Беляева Т.М. и др. Информационные технологии в юридической деятельности: учеб. / под ред. В.Д. Элькина. М.: Проспект, 2013. 349 с.

3. Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 163.

4. Мешалкин С.Н., Горностаева И.В., Федоткин А.И. Выявление, предупреждение, раскрытие и расследование преступлений экстремистской направленности, совершаемых в сети Интернет: учеб.-метод. пособие // Труды сотрудников Всероссийского института повышения квалификации сотрудников МВД России. Домодедово: ВИПК МВД России, 2016. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

5. Пинкевич Т.В., Смольянинов Е.С. Международный опыт противодействия преступной деятельности с использованием криптовалюты: учеб.-практич. пособие. М.: Академия управления МВД России, 2021. 108 с. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

6. Бегишев И.Р., Бикеев И.И. Преступления в сфере обращения цифровой информации. Сер. Цифровая безопасность. Казань: Изд-во «Познание» Казанского инновационного университета, 2020. 300 с.

2. ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ КАК ОСНОВА ВЫЯВЛЕНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ

Тема 2.1. Понятие и сущность оперативно-розыскной деятельности

Место и роль оперативно-розыскной деятельности в государственной системе мер борьбы с преступностью

Вопросы общей теории оперативно-розыскной деятельности (ОРД), ее методология имеют огромное значение для качественного улучшения оперативно-розыскной практики борьбы с преступностью в современных условиях. Более того, в специальной литературе было подчеркнуто ее исключительное значение в доказательственном обеспечении предварительного расследования и судебного разбирательства по уголовным делам¹. Сам термин «оперативно-розыскная деятельность» означает быстрый, гласный или негласный поиск информации о лицах и фактах, представляющих оперативный интерес для решения задач борьбы с преступностью.

Системой мер борьбы с преступностью от имени государства являются положения действующего уголовного, уголовно-процессуального, административного законодательства и другие нормативные правовые акты.

Уголовное право как отрасль российского права представляет систему юридических норм, характеризующих общественно опасные деяния как преступления и устанавливающих наказание за их совершение. Уголовный процесс представляет собой систему юридических норм, регулирующих деятельность правоохранительных органов по расследованию, рассмотрению и разрешению уголовных дел. Административное право регулирует правоотношения в области выявления административных правонарушений и соответственно применяет к виновным меры административного воздействия. Криминалистика – наука, разрабатывающая систему специальных приемов, методов и средств собирания, фиксации, исследования и использования судебных доказательств. Криминология – наука, изучающая закономерности существования и

¹ Основы оперативно-розыскной деятельности: учеб. / под ред. В.Б. Рушайло. СПб., 2000. С. 62–64; Оперативно-розыскная деятельность: учеб. / под ред. К.К. Горяинова, В.С.Овчинского, А.Ю. Шумилова. М.: ИНФРА-М, 2001. XXII. С. 302; Основы оперативно-розыскной деятельности органов внутренних дел: учеб. / под общ. ред. Ю.А. Агафонова, Ю.Ф. Кваши. Краснодар: Кру МВД РФ. 2008. С. 34; Маркушин А.Г. Оперативно-розыскная деятельность: учеб. для вузов. М., 2012. С. 13.

развития преступности, а также более широкого круга общественных явлений и процессов, связанных с ней.

Однако ни одна из вышеуказанных юридических дисциплин не дает ответа на вопрос, в отношении кого инкриминировать преступление, кого привлекать к уголовной ответственности и наказанию, чьи следы необходимо обнаружить и исследовать, в отношении кого проводить следственные действия и судебные разбирательства. На эти и другие вопросы отвечает теория ОРД. Сущность ОРД составляет ее поисковая направленность: деятельность оперативных аппаратов нацелена на *поиск информации* о лицах, подготавливающих, совершающих и совершивших преступления, иных лицах и фактах, представляющих оперативный интерес.

Оперативно-розыскная деятельность представляет собой специфическую разновидность правоохранительной деятельности, которая осуществляется посредством проведения таких оперативно-розыскных мероприятий, как опрос; наведение справок; сбор образцов для сравнительного исследования; проверочная закупка; исследование предметов и документов; отождествление личности; обследование помещений, зданий, сооружений, участков местности и транспортных средств (оперативный осмотр); контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических каналов связи; оперативное внедрение; контролируемая поставка; оперативный эксперимент; получение компьютерной информации (ч. 1 ст. 6 ФЗ «Об ОРД»).

Вышеперечисленные ОРМ представляют собой способы добывания и проверки информации, необходимой для решения задач ОРД. Разведывательный (оперативно-розыскной) характер они приобретают за счет сочетания с методами конспирации, т. е. способами, применяемыми оперативными подразделениями для сохранения в тайне их деятельности, а также создания у объектов ОРД ложных представлений о действительных участниках, сущности и достигаемых результатах ОРМ.

Место и роль ОРД в государственной системе мер борьбы с преступностью заключается в том, что раскрытие преступлений, обнаружение лиц, их совершивших, и иных разыскиваемых лиц целиком ложится на оперативные подразделения органов, осуществляющих ОРД. Законодательство четко разделяет полномочия органов предварительного расследования и органов, осуществляющих ОРД, на которые возложена обязанность *выявлять латентные преступления и раскрывать совершенные в условиях неочевидности*. Подготовка и совершение преступлений осуществляются скрытно, изоэтно, замаскированно, поэтому применяемые сотрудниками органов внут-

ренных дел оперативно-розыскные меры тоже должны быть замаскированными, скрытными, разведывательными. В теории ОРД присутствует единодушие по поводу необходимости использования в первую очередь негласных мер¹.

Нормы ФЗ «Об ОРД» содержат предписания, направленные на противодействие не только преступлениям, но и административным правонарушениям. Многие ОРМ (опрос, наведение справок, сбор образцов для сравнительного исследования, осмотр транспортных средств и др.) проводятся сотрудниками полиции и в целях выявления и пресечения административных правонарушений.

Оперативно-розыскная деятельность направлена не только на борьбу с преступностью, но и на сбор информации в отношении широкого круга проверяемых лиц. Так, ч. 2, 3 ст. 7 ФЗ «Об ОРД» дает право на проведение ОРМ, направленных не только на противодействие уголовным и административным правонарушениям, но также и на проверку лиц, допущенных к осуществлению ОРД, государственной тайне, работам, связанным с эксплуатацией экологически опасных объектов, либо сбора информации в отношении должностных лиц в соответствии с ФЗ «О противодействии коррупции» и др. Тем самым законодатель закрепил за ОРД возможность вторгаться в личную и общественную деятельность человека.

Законодательное определение ОРД как особого вида правоохранительной деятельности и ее признаки

Первая статья ФЗ «Об ОРД» определяет ОРД как «вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом в пределах их полномочий, посредством проведения ОРМ и в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств».

Оперативно-розыскная деятельность в первую очередь направлена на сбор информации о лицах и фактах, представляющих оперативный интерес. Ее проводят в пределах своей компетенции должностные лица государственных правоохранительных органов.

Признаки, присущие ОРД

1. Оперативно-розыскная деятельность – это самостоятельный вид деятельности. Федеральный закон «Об ОРД» – единственный в

¹ Маркушин А.Г. Оперативно-розыскная деятельность: учеб. для вузов. М., 2012. С. 14; Дубоносов Е.С. Оперативно-розыскная деятельность: учеб. для вузов. М., 2013. С. 48–49.

своем роде законодательный нормативный акт органов государственной власти, который дал право спецслужбам решать задачи борьбы с преступностью, используя как гласные, так и негласные методы и применяя при этом специальные технические средства. Гласные методы представляют собой деятельность оперативных подразделений полиции, направленную на подготовку и проведение гласных ОРМ, при этом используется гласное содействие отдельных граждан и специалистов. К негласным методам относятся использование конфиденциального содействия граждан при подготовке и проведении негласных ОРМ. Негласные методы, применяемые в ОРД, строятся на принципе конспирации, который предполагает неразглашение сведений о силах, средствах, источниках, методах, планах и результатах ОРД, о лицах, внедренных в организованные преступные группы, штатных негласных сотрудниках, лицах, оказывающих конфиденциальное содействие, а также об организации и тактике проведения ОРМ.

2. Оперативно-розыскная деятельность реализуется путем собственных только ей ОРМ, характеризующихся определенной организационно-упорядоченной формой. Перечень ОРМ, основание, условия их проведения и оформление результатов приведены в гл. 2 ФЗ «Об ОРД». Оперативно-розыскные мероприятия направлены в первую очередь на решение задач ОРД и состоят в собирании информации о подготавливаемом, совершенном, совершаемом преступлении и лицах, их подготавливающих или совершивших. Результаты, полученные в ходе проведения ОРМ, могут использоваться в доказывании по уголовным делам, являться поводом и основанием для возбуждения уголовного дела, представляться органу дознания, следователю или в суд, в производстве которого находится уголовное дело.

3. Оперативно-розыскная деятельность направлена в основном на борьбу с преступностью (ст. 2, ч. 1 ст. 5 ФЗ «Об ОРД») и осуществляется в форме выявления лиц и фактов, представляющих оперативный интерес, оперативно-розыскной профилактики и оперативной проверки. Должностные лица органов, осуществляющих оперативно-розыскную деятельность, для решения задач ОРД могут создавать и использовать информационные системы, а также заводить дела оперативного учета (ДОУ). Информационно-поисковые системы, находящиеся в АБД информационных центров МВД России и субъектов Российской Федерации, состоят из оперативно-справочных, криминалистических, розыскных учетов, коллекций и картотек и регламентируются нормативными актами МВД России.

4. Оперативно-розыскная деятельность имеет четкую оперативно-поисковую направленность и выражается в поиске информации о

лицах и фактах, представляющих оперативный интерес. Информацию получают на месте происшествия, при опросе свидетелей и очевидцев, в результате привлечения к конфиденциальному содействию лиц, которые могут предоставлять оперативно значимую информацию, при изучении финансовых и иных хозяйственных документов, а также в отношении лиц отрицательной направленности, отбывающих уголовное наказание и др.

5. Оперативно-розыскные мероприятия проводятся должностными лицами органов, осуществляющих ОРД от имени государства и только на правовой основе. Перечень органов, уполномоченных на осуществление ОРД, дается в ст. 13 ФЗ «Об ОРД», а других должностных лиц – в Федеральном законе «О полиции» и других подзаконных нормативных актах. Оперативно-розыскные мероприятия проводятся в соответствии с ФЗ «О полиции» и ведомственными нормативными актами МВД России¹.



¹ О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: приказ МВД России от 19.07. 2012 № 608».

Вопросы для самостоятельного изучения

1. История становления уголовного розыска полиции России.
2. Оперативно-розыскная деятельность в отечественной и зарубежной литературе и кинематографии.

Примерный план занятия

1. Место и роль оперативно-розыскной деятельности в государственной системе мер борьбы с преступностью.
2. Социально-историческая обусловленность возникновения и объективная необходимость существования ОРД на современном этапе.
3. Законодательное определение ОРД как особого вида правоохранительной деятельности и ее признаки.

Вопросы для самоконтроля по теме

1. Определение оперативно-розыскной деятельности в соответствии со ст. 1 ФЗ «Об ОРД».
2. Цели оперативно-розыскной деятельности.
3. Признаки оперативно-розыскной деятельности.

Тема 2.2. Задачи и принципы оперативно-розыскной деятельности

Цель ОРД, согласно ст. 1 ФЗ «Об ОРД», – гарантия защиты от потенциальной опасности для общества и государства, а также защиты от разного вида посягательств: на жизнь, здоровье, собственность, права и свободы гражданина.

Для обеспечения защиты от посягательств на вышеуказанные объекты создана структура оперативно-розыскных, организационных, правовых и иных мер. В обязанности лиц, осуществляющих ОРД, входит не только гарантия защиты в случае опасности общества и государства, но и устранение мотивов и обстоятельств совершения злодеяний.

Защита собственности осуществляется государством при помощи оперативно-розыскных мер. В соответствии с ч. 2 ст. 8 Конституции РФ форма собственности (частная, государственная, муниципальная) не влияет на степень защиты. Последняя предполагает обеспечение оперативно-розыскными силами и средствами неприкосновенности, а в случае нанесения вреда преступным действием – принятие мер по возмещению материального ущерба.

Защита России от внешних и внутренних преступных посягательств также является целью ОРД. Однако те посягательства, которые не считаются преступлением, находятся вне юрисдикции оперативно-розыскных органов.

Личность, общество и государство относятся к основным объектам государственной защиты. Защита личности подразумевает обеспечение конституционных прав, свобод, а также достойного уровня и качества жизни граждан. Защита общества – это защита его материальных и духовных ценностей. В государстве защите подлежат независимость, конституционный строй, устойчивое развитие и территориальная целостность. Государство, являясь основным институтом политической системы общества, управляет последним и обеспечивает его безопасность. Данные условия способствуют эффективному функционированию и развитию государства.

Частью внутренней и внешней политики Российской Федерации в сфере обеспечения безопасности является государственная политика. Она состоит из комплекса согласованных и объединенных общим замыслом мер (политических, военных, социально-экономических, правовых, информационных, организационных и др.).

Самостоятельно безопасность как состояние объекта не может возникнуть. Ее обеспечивает либо сам объект, либо уполномоченные государственные органы. К числу органов, обеспечивающих безопасность, относятся силы с предусмотренной федеральным законодательством военной или правоохранительной службой. Таким образом, термин «безопасность» приобретает смысл только при наличии мер государственной защиты. Федеральная служба безопасности России, МВД России, ФСО России, СВР и другие органы, которые осуществляют ОРД, имеют в своем арсенале меры государственной защиты.

Осуществление ОРД для решения задач и достижения целей не допускается в случае, если какие-либо действия противоречат ФЗ «Об ОРД» (ч. 2 ст. 5). Данное воспрещение во время проведения ОРМ подтверждает соблюдение прав и свобод человека на неприкосновенность его частной жизни и жилища, а также на неразглашение личной и семейной тайны.

Под принципами ОРД понимаются основополагающие начала, руководящие идеи, отражающие убеждения и взгляды общества в лице его законодательных и правоохранительных органов на сущность, цели и задачи этой специфической государственно-правовой формы борьбы с преступностью. Принципы ОРД сформировались в процессе практической деятельности оперативных подразделений органов внутренних дел, были обобщены и сформулированы теорией ОРД и получили нормативное закрепление в действующем законодательстве и ведомственном правовом регулировании. Принятие ФЗ «Об ОРД» придало принципам ОРД статус законодательных норм с соответствующим механизмом их реализации

В ст. 3 ФЗ «Об ОРД» закреплены четыре основных принципа ОРД. Принципы законности, уважения и соблюдения прав и свобод человека и гражданина традиционно относятся к общеправовым принципам, характерным для всех отраслей права. Их закрепление в законе обусловлено, во-первых, спецификой правовых основ ОРД, до недавнего времени регламентировавшейся только ведомственными нормативными актами, во-вторых, тем, что сущность ОРД предполагает некоторые ограничения конституционных прав и свобод граждан, попавших в ее сферу. Принципы конспирации и сочетания гласных и негласных методов и средств неизвестны другим отраслям права, поэтому их относят к специальным (отраслевым) принципам оперативно-розыскной деятельности.

Задачи оперативно-розыскной деятельности



Принципы оперативно-розыскной деятельности



Примерный план занятия

1. Задачи ОРД, закрепленные в ФЗ «Об ОРД».
2. Содержание задач ОРД и их сущность.
3. Принципы ОРД, закрепленные в ФЗ об ОРД, отражающие закономерности борьбы с преступностью.
4. Система принципов ОРД и ее взаимосвязанная структура.
5. Общие и специальные принципы ОРД.
6. Связь и соотношение общих и специальных принципов ОРД.

Вопросы для самоконтроля по теме

1. Назовите общие задачи оперативно-розыскной деятельности.
2. Назовите специальные задачи оперативно-розыскной деятельности.
3. Назовите общие принципы оперативно-розыскной деятельности.
4. Назовите специальные принципы оперативно-розыскной деятельности.

Тема 2.3. Правовое регулирование оперативно-розыскной деятельности

В общей теории права совокупность нормативных актов, касающихся какой-либо области общественных отношений, охватывается категорией источников права. Однако в ОРД такую совокупность нормативных актов принято называть ее правовой основой. Правовую основу ОРД составляют нормативные акты, в содержании которых имеются правовые нормы, непосредственно касающиеся ее назначения, организации и регламентации.

В соответствии со ст. 4 ФЗ «Об ОРД» правовую основу ОРД составляют:

- Конституция Российской Федерации;
- Федеральный закон «Об оперативно-розыскной деятельности»;
- другие федеральные законы и законы Российской Федерации, имеющие отношение к регламентации оперативно-розыскной деятельности;
- иные нормативные правовые акты федеральных органов государственной власти.

В Конституции РФ содержится ряд положений, непосредственно касающихся ОРД. В гл. 2 Конституции РФ содержатся нормы, касающиеся прав и свобод личности: в соответствии с ч. 2 данной статьи каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. На основании ст. 25 Конституции РФ жилище неприкосновенно: никто не вправе проникать в жилище против воли проживающих в нем лиц и иначе как в случаях, прямо установленных Федеральным законом и на основании судебного решения. В соответствии с ч. 1 ст. 46 Основного Закона каждому гарантируется судебная защита его прав и свобод. При этом в соответствии с ч. 3 ст. 55 Конституции РФ права и свободы личности могут быть ограничены Федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Правовые и организационные основы ОРД изложены шести главах ФЗ «Об ОРД», включающих в себя 23 статьи. В первой главе определяется сущность ОРД, ее задачи и принципы, правовая основа, а также гарантии соблюдения прав и свобод человека и гражданина при осуществлении ОРД. Вторая глава посвящена проведению ОРМ.

В ней приводится система ОРМ, основания и условия их проведения, основания и порядок судебного рассмотрения материалов об ограничении конституционных прав личности при проведении ОРМ. Ряд статей касаются информационного обеспечения и документирования в ОРД, использования ее результатов в уголовном судопроизводстве. В третьей главе определены органы, осуществляющие ОРД, перечислены их полномочия. Отдельная статья посвящена социальной и правовой защите должностных лиц, наделенных оперативно-розыскными полномочиями. Четвертая глава посвящена правовым основам содействия граждан органам, осуществляющим ОРД, включая их социальную и правовую защиту. В пятой главе определяются правовые и организационные основы финансового обеспечения ОРД. Вопросы контроля и надзора за оперативно-розыскной деятельностью представлены в нормах шестой главы. Положения ФЗ «Об ОРД» представляют собой базу ведомственных нормативных актов, непосредственно регламентирующих организацию и тактику ОРД.

К другим федеральным законам, имеющим непосредственное отношение к правовой основе ОРД, следует отнести законы, регулирующие общественные отношения, возникающие и действующие в сфере ОРД. Их можно подразделить на три группы:

- законы, устанавливающие основные положения осуществления ОРД;
- законы, регламентирующие деятельность отдельных субъектов ОРД;
- законы, регулирующие отношения, возникающие при решении частных задач частных задач ОРД.

Первая группа представлена Уголовным кодексом РФ, Уголовно-процессуальным кодексом РФ, законами РФ «О государственной тайне», «О безопасности» и ФЗ «О прокуратуре Российской Федерации».

Ко второй группе относятся: Уголовно-исполнительный кодекс РФ, Таможенный кодекс таможенного союза, Закон РФ «Об учреждениях и органах, исполняющих наказания в виде лишения свободы», федеральные законы «О полиции», «Об органах Федеральной службы безопасности в Российской Федерации», «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений», «О внешней разведке», «О государственной охране», «О прокуратуре Российской Федерации», «О следственном комитете Российской Федерации» и некоторые другие.

Третью группу составляют: Гражданский кодекс РФ, ФЗ «О наркотических средствах и психотропных веществах», законы

Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации», «О средствах массовой информации», федеральные законы «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов», «О связи», «Об информации», «О банках и банковской деятельности», «О борьбе с терроризмом», «О противодействии коррупции» и др.

К иным нормативным правовым актам федеральных органов государственной власти как составной части правовой основы ОРД можно отнести:

- указы Президента РФ (например, УПРФ: от 30 ноября 1995 г. № 1203 «Перечень сведений, отнесенных к государственной тайне», от 1 сентября 1995 г. № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств», от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации», от 18 апреля 1996 г. № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью», от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера», от 19 мая 2008 г. № 815 «О мерах по противодействию коррупции» и др.;

- постановления Правительства РФ (от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности», от 28 октября 1995 г. № 1050 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», от 1 июля 1996 г. № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств (разработанных, приспособленных, запрограммированных) для негласного получения информации» (сюда включен также «Перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления ОРД»), утвержденное этим же постановлением, от 27 августа 2005 г. № 538 «Об утверждении Пра-

вил взаимодействия операторов связи с уполномоченными органами, осуществляющими оперативно-розыскную деятельность» и др.;

– нормативные акты органов, осуществляющих ОРД, регламентирующие организацию и тактику проведения ОРМ.

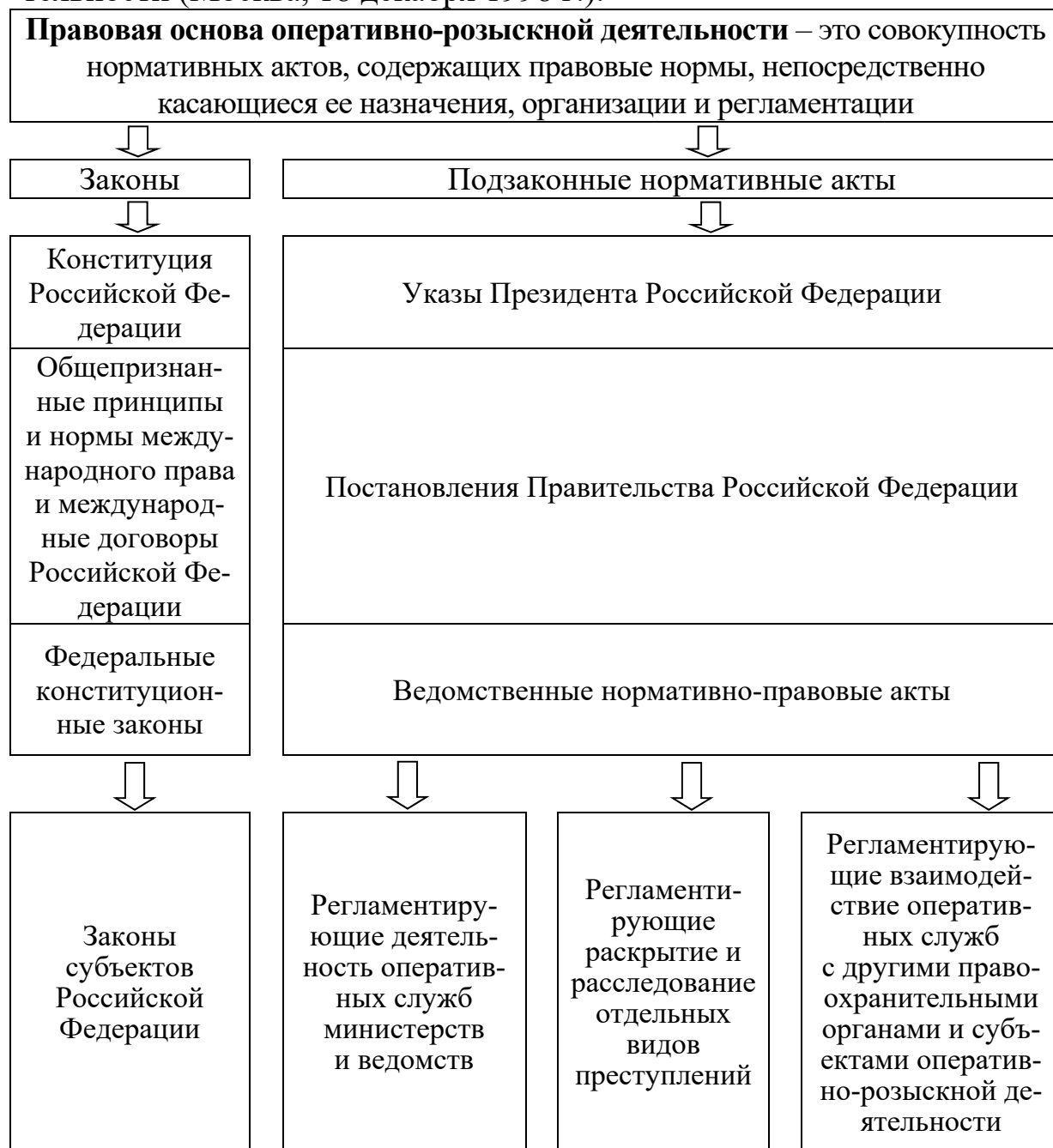
В соответствии с ч. 1 ст. 12 ФЗ «Об ОРД» сведения об организации и тактике ОРД составляют государственную тайну. В связи с этим рассматриваемая группа нормативных актов издается с соответствующими грифами секретности и доступ к ним имеют только сотрудники и руководители оперативных подразделений, а также должностные лица государственных органов, осуществляющие контроль и надзор за ОРД, при наличии допуска к сведениям, составляющим государственную тайну.

Руководители министерств и ведомств, осуществляющих ОРД, издают также несекретные нормативные акты, касающиеся ОРД, к которым, в частности, относятся: Инструкция о порядке представления результатов ОРД органу дознания, следователю или в суд (утверждена Приказом МВД России, МО России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68); Инструкция по организации информационного обеспечения сотрудничества по линии Интерпола (утверждена приказами МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС России от 6 октября 2006 г. № 786/310/470/454/333/971, в редакции приказа МВД РФ № 727, Минюста РФ № 302, ФСБ РФ № 480, ФСО РФ № 570, ФСКН РФ № 425, ФТС РФ № 1739 от 22 сентября 2009 г.) и др.

В соответствии с ч. 4 ст. 15 Конституции РФ в правовую основу ОРД входят также международные правовые акты, касающиеся борьбы с преступностью. Часть 4 ст. 7 ФЗ «Об ОРД» рассматривает запросы международных правоохранительных организаций в качестве самостоятельного основания проведения ОРМ, а п. 3 ст. 14 обязывает оперативные подразделения исполнять запросы правоохранительных органов иностранных государств.

Наиболее значимые международные правовые акты, имеющие отношение к ОРД: Всеобщая декларация прав человека, принятая Генеральной Ассамблеей ООН 10 декабря 1948 г.; Международный пакт о гражданских и политических правах, принятый Генеральной Ассамблеей ООН 16 декабря 1966 г.; Европейская конвенция о защите прав человека и основных свобод, принятая Советом Европы 4 ноября 1950 г.; Европейская конвенция о взаимной правовой помощи по уголовным делам, принятая Советом Европы 20 апреля 1959 г.; Конвен-

ция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Минск, 22 января 1993 г.); Соглашение о взаимодействии министерств внутренних дел независимых государств в сфере борьбы с преступностью (Алма-Ата, 24 апреля 1992 г.); Соглашение о сотрудничестве между министерствами внутренних дел в борьбе с незаконным оборотом наркотических средств и психотропных веществ (Киев, 21 октября 1992 г.); Соглашение о сотрудничестве министерств внутренних дел в сфере борьбы с организованной преступностью (Ашхабад, 17 февраля 1994 г.); Соглашение о сотрудничестве в сфере специального сопровождения оперативно-розыскной деятельности (Москва, 18 декабря 1998 г.).



Примерный план занятия

1. Понятие, сущность и необходимость правового регулирования ОРД.
2. Система правового регулирования ОРД.
3. Положения Конституции РФ в основе системы правового регулирования.
4. Общепризнанные принципы и нормы международного права в системе правового регулирования.
5. Федеральные законы в правовом регулировании ОРД.
6. Общая характеристика Закона «Об ОРД». Связь и соотношение норм права, регулирующих ОРД, и ведомственных нормативных актов.

Вопросы для самоконтроля по теме

1. Структура и содержание ФЗ «Об ОРД».
2. Назовите положения Конституции РФ, связанные с ОРД.
3. Что относится к подзаконным нормативным правовым актам, регулирующим ОРД.

Тема 2.4. Соблюдение прав и свобод человека и гражданина при осуществлении оперативно-розыскной деятельности

Понятие и значение конституционных прав и свобод человека и гражданина в оперативно-розыскной деятельности

В определении Конституционного суда РФ от 15 июля 2004 г. № 304-0 говорится о допустимости в конституционно значимых целях возможности соразмерного ограничения федеральным законом прав и свобод человека и гражданина. Ограничение прав и свобод граждан предусмотрено в ФЗ «Об ОРД» в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

При ограничении прав человека и гражданина в процессе ОРД обязательно соблюдение следующих требований:

- 1) допустимость ограничения определенных прав и свобод человека и гражданина Конституцией РФ (ч. 2 ст. 23, ст. 25, ч. 3 ст. 55 и др.);
- 2) соблюдение требований оперативно-розыскного законодательства относительно оснований и условий ограничения прав и свобод (полномочия субъектов, ограничивающих права, оформление ими проводимых ОРМ, необходимость санкционирования судом и др.);
- 3) выполнение временных параметров ограничений и их соразмерность, т. е. возможность их применения на период противоправной деятельности лица и с учетом общественной опасности подготавливаемого, совершаемого или совершенного преступления.

В процессе проведения ОРМ законодательством предусмотрено *ограничение следующих прав*:

- на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ч. 1 ст. 23, ч. 1 ст. 24 Конституции РФ);
- тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23 Конституции РФ, ч. 2 ст. 8 ФЗ «Об ОРД»);
- неприкосновенность жилища (ст. 25 Конституции РФ, ч. 2 ст. 8 ФЗ «Об ОРД»).

Перечисленные права могут быть ограничены при проведении таких ОРМ, как наблюдение (негласное наружное, электронное, осуществляемое внутри помещения); прослушивание телефонных переговоров; снятие информации с технических каналов связи; негласное обследование помещений, зданий, сооружений, участков местности,

транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; и др.

Конституция РФ в ст. 24 устанавливает общее правило, запрещающее сбор, хранение и распространение информации о частной жизни лица без его согласия. Однако данное право может быть ограничено в процессе осуществления ОРМ, так как преступное деяние не относится к сфере частной жизни.

Сведения, затрагивающие неприкосновенность частной жизни, могут предаваться огласке без согласия граждан в случаях, предусмотренных федеральным законом, например, если они являются предметом свидетельских показаний.

Ограничение права на неприкосновенность жилища допускается только в случаях, установленных федеральным законом, или на основании судебного решения (ст. 25 Конституции РФ).

Не является нарушением неприкосновенности жилища проведение ОРМ, сопряженное с входением в него с согласия хотя бы одного из проживающих в нем лиц либо входением в помещение гостиницы, санатория, пансионата, дома отдыха в присутствии администрации этих учреждений, если это предусмотрено правилами проживания, внутреннего распорядка, договорами.

Ограничение права на неприкосновенность жилища допускается ФЗ «О полиции» (ч. 3 ст. 15), в соответствии с которым допускается проникновение сотрудников полиции в жилые и иные помещения, на земельные участки и территории (за исключением помещений, земельных участков и территорий дипломатических представительств и консульских учреждений иностранных государств, представительств международных организаций):

1) для спасения жизни граждан и (или) их имущества, обеспечения безопасности граждан или общественной безопасности при массовых беспорядках и чрезвычайных ситуациях;

2) задержания лиц, подозреваемых в совершении преступления;

3) пресечения преступления;

4) установления обстоятельств несчастного случая.

Соблюдение прав и свобод человека и гражданина при проведении оперативно-розыскного мероприятия

Органы, осуществляющие ОРД, располагают бóльшим арсеналом ограничений прав граждан по сравнению с теми, которые применяются в уголовном процессе, административном праве. Но в отличие от последних эти ограничения носят скрытый от граждан характер.

Несмотря на это, в процессе ОРД существует механизм соблюдения прав и законных интересов личности при осуществлении ОРМ.

Соблюдение прав и свобод человека при проведении ОРМ как одна из форм реализации права предполагает воздержание субъектов ОРД от совершения неправомерных действий, запрещенных оперативно-розыскным законодательством.

Соблюдение прав и свобод при осуществлении ОРМ обеспечивается:

1) соблюдением субъектами ОРД неприкосновенности частной жизни, личной и семейной тайны, неприкосновенности жилища и тайны корреспонденции (ч. 1 ст. 24 Конституции РФ); запрет на разглашение таких сведений содержится ч. 8 ст. 5 ФЗ «Об ОРД»;

2) недопущением осуществления ОРД для достижения целей и решения задач, не предусмотренных ФЗ «Об ОРД»;

3) запретом на осуществление действий, прямо запрещенных законом (ч. 8 ст. 5 ФЗ «Об ОРД»).

Правовой гарантией соблюдения прав и законных интересов личности при проведении ОРМ является установление уголовной ответственности за нарушение неприкосновенности частной жизни (ст. 137 УК РФ), тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), неприкосновенности жилища (ст. 139 УК РФ).

Органам, осуществляющим ОРД, запрещается:

- проводить ОРМ в интересах какой-либо политической партии, общественного или религиозного объединения;

- принимать негласное участие в работе федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, а также в деятельности зарегистрированных в установленном порядке и незапрещенных политических партий, общественных и религиозных объединений в целях оказания влияния на характер их деятельности;

- разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя гражданина и которые стали известны в процессе проведения ОРМ, без согласия граждан, за исключением случаев, предусмотренных федеральными законами;

- подстрекать, склонять, побуждать в прямой или косвенной форме к совершению противоправных действий (провокация);

- фальсифицировать результаты ОРД.

Лица, оказывающие конфиденциальную помощь, обязаны сохранять в тайне сведения, ставшие им известными в ходе проведения ОРМ (ч. 1 ст. 17 ФЗ «Об ОРД»).

При защите жизни и здоровья граждан, их конституционных прав и законных интересов, а также для обеспечения безопасности общества и государства от преступных посягательств допускается вынужденное причинение вреда правоохраняемым интересам должностным лицом органа, осуществляющего ОРД, либо лицом, оказывающим ему содействие, совершаемое при правомерном выполнении указанным лицом своего служебного или общественного долга.

Вместе с соблюдением прав и свобод граждан, указанных в ст. 5, ФЗ «Об ОРД» в ст. 16 обеспечил социальную и правовую защиту должностных лиц, органов, осуществляющих ОРД, и при этом установил, что никто не вправе вмешиваться в законные действия должностных лиц и органов, осуществляющих ОРД, за исключением лиц, прямо уполномоченных на то федеральными законами.

Должностное лицо, уполномоченное на осуществление оперативно-розыскной деятельности, в ходе проведения ОРМ подчиняется только непосредственному и прямому начальнику. При получении приказа или указания, противоречащего закону, указанное должностное лицо обязано руководствоваться законом.

Основания и порядок обжалования гражданами действий должностных лиц, уполномоченных на осуществление оперативно-розыскной деятельности

Защита прав и свобод человека и гражданина обеспечивается:

- 1) возможностью обжалования гражданином незаконных ОРМ, которые нарушили его права, законные интересы и причинили вред;
- 2) возможностью истребования информации из оперативно-розыскного органа (ч. 4 ст. 5 ФЗ «Об ОРД»);
- 3) ведомственным, судебным контролем и прокурорским надзором над ОРД.

Право на обжалование гражданином незаконных (по его мнению) ОРМ в первую очередь распространяется на случаи нарушения основных конституционных прав и свобод граждан: на достоинство личности (ст. 21 Конституции РФ), неприкосновенность частной жизни, личную и семейную тайну (ч. 1 ст. 23), тайну переписки и телефонных переговоров (ч. 2 ст. 23), неприкосновенность жилища (ст. 25) и некоторых других. Могут быть обжалованы и случаи нарушения ряда специфических прав, которыми наделяются граждане,

оказывающие содействие правоохранительным органам на конфиденциальной основе.

Право на обжалование, как указано в п. 2 определения Конституционного суда РФ от 14 июля 1998 г. № 86-0, возникает у граждан, даже если они только полагают, что действия должностных лиц оперативных аппаратов привели к нарушению их прав и свобод.

Действия должностных лиц, осуществляющих ОРД, могут быть обжалованы в *три инстанции*: а) вышестоящий орган; б) прокуратуру; в) суд.

Вышестоящий орган в соответствии с ч. 2 ст. 4 Закона РФ от 27 апреля 1993 г. № 4866-1 «Об обжаловании в суд действий и решений, нарушающих права и свободы граждан» обязан рассмотреть жалобу в месячный срок.

Порядок рассмотрения жалоб, заявлений граждан в органы, осуществляющие ОРД, регламентируется ведомственными подзаконными актами.

Граждане могут записаться на прием к руководителю ОВД или его заместителю. Все поступившие жалобы граждан регистрируются в специальном журнале, руководитель определяет сроки и исполнителей проверки жалобы. Запрещается направлять жалобы граждан для разрешения тем органам и должностным лицам, действия которых обжалуются. По результатам проверки жалобы составляется мотивированное заключение, в котором указываются принятые меры по восстановлению нарушенных прав.

После проверки жалобы заявителю должен быть дан письменный ответ. Если гражданину в удовлетворении жалобы отказано или он не получил ответа в течение месяца со дня ее подачи, он вправе обратиться с жалобой в суд.

Жалоба в прокуратуру подается по месту жительства заявителя или по месту нахождения органа, на который подается жалоба. Порядок и сроки ее рассмотрения определяются ФЗ от 20 января 1992 г. № 2201-1 «О прокуратуре Российской Федерации».

Генеральный прокурор рекомендует рассматривать жалобы и заявления на нарушения конституционных прав граждан в пятидневный срок. Если в указанный срок разрешить жалобу или заявление не представляется возможным, заявителю направляется уведомление о сроке разрешения его жалобы. После проведенной проверки прокурор дает ответ на жалобу (заявление). В случае отказа в удовлетворении жалобы гражданину должен быть разъяснен порядок обжалования принятого решения.

Незаконные действия оперативно-розыскных органов могут быть обжалованы и Уполномоченному по правам человека РФ, что предусмотрено Федеральным конституционным законом от 26 февраля 1997 г. № 1-ФКЗ «Об Уполномоченном по правам человека в Российской Федерации».

Предметом судебного разбирательства чаще всего является не законность проведения ОРМ, не возмещение причиненного вреда, а обоснованность ограничения конституционного права гражданина на ознакомление с документами и материалами, непосредственно затрагивающими его права и свободы. Обжалование в суд отказа в предоставлении сведений о полученной в отношении лица информации может быть соединено в одном производстве с обжалованием действий органов, осуществляющих ОРД, и с иском о возмещении причиненного вреда.

Судья, рассматривающий жалобу, не вправе самостоятельно знакомить заявителя с полученными оперативно-служебными документами, излагать ему их содержание в связи с тем, что документы могут содержать сведения, относимые к государственной тайне. Решение суда направляется руководителю субъекта ОРД, действия которого были обжалованы, либо вышестоящему органу.

Гражданско-правовая ответственность наступает при рассмотрении судом жалобы гражданина и признании незаконными действий оперативно-розыскного органа. К мерам воздействия, которые могут быть при этом применены, относятся возмещение имущественного ущерба и возмещение морального вреда.

Постановка вопроса о возмещении имущественного ущерба и морального вреда возможна в случаях, когда действия сотрудников противоречат основаниям и условиям осуществления ОРМ. В этом случае по заявлению пострадавшего либо прокурора, если потерпевший не в состоянии это сделать сам, возбуждается исковое производство и разрешается вопрос об ответственности конкретного лица, причинившего имущественный ущерб или моральный вред, а также о компенсации потерь, понесенных потерпевшим. Эти вопросы разрешаются в соответствии со ст. 12, 150, 1069 ГК РФ.

Примерный план занятия

1. Понятие и значение конституционных прав и свобод человека и гражданина в ОРД.
2. Соблюдение прав и свобод человека и гражданина при проведении ОРМ.

3. Основания и порядок обжалования гражданами действий должностных лиц, уполномоченных на осуществление ОРД.

Вопросы для самоконтроля по теме

1. Какие права граждан могут быть ограничены в процессе проведения ОРМ в соответствии с законодательством РФ?

2. В соответствии со ст. 5 ФЗ «Об ОРД» каким образом обеспечиваются конституционные права и свободы человека и гражданина?

3. Что запрещается органам, осуществляющим ОРД?

4. В какие инстанции могут быть обжалованы действия должностных лиц, осуществляющих ОРД?

Тема 2.5. Государственные органы и должностные лица, осуществляющие оперативно-розыскную деятельность, их обязанности и права

Органы, осуществляющие оперативно-розыскную деятельность

В статье 13 ФЗ «Об ОРД» приведен перечень органов, оперативным подразделениям которых предоставлено право осуществлять ОРД на территории Российской Федерации: органы внутренних дел, ФСБ России, Федеральные органы государственной охраны, таможенные органы РФ, СВР России, ФСИН России.

Такие подразделения и их сотрудники являются субъектами, осуществляющими ОРД.

Органы, осуществляющие ОРД, решают определенные ФЗ «Об ОРД» задачи исключительно в пределах своих полномочий, установленных соответствующими законодательными актами Российской Федерации. Руководители указанных органов подзаконными ведомственными нормативными правовыми актами (как правило, закрытого характера) определяют перечень входящих в них оперативных подразделений, их полномочия, структуру и организацию работы.

Оперативные подразделения органов службы внешней разведки проводят ОРМ только в целях обеспечения их собственной безопасности и в случае, если проведение этих мероприятий не затрагивает полномочий органов, осуществляющих ОРД в полном объеме.

Оперативные подразделения указанных органов вправе проводить с работниками уголовно-исполнительной системы ОРМ в следственных изоляторах этой системы.

Задачи оперативных подразделений ОВД:

- выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших;
- осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыска без вести пропавших;
- установление имущества, подлежащего конфискации.

Основными направлениями деятельности *органов ФСБ* являются: контрразведывательная деятельность; борьба с терроризмом, борьба с преступностью, разведывательная деятельность, пограничная деятельность, обеспечение информационной безопасности.

В соответствии со ст. 9 ФЗ «О федеральной службе безопасности» под контрразведывательной деятельностью понимается деятель-

ность по выявлению, предупреждению, пресечению разведывательной и иной деятельности специальных служб и организаций иностранных государств, а также отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации.

Согласно ст. 10 ФЗ «О федеральной службе безопасности» оперативные подразделения ФСБ осуществляют ОРМ по выявлению, предупреждению, пресечению и раскрытию шпионажа, террористической деятельности, организованной преступности, коррупции, незаконного оборота оружия и наркотических средств, контрабанды и других преступлений, дознание и предварительное следствие по которым отнесены законом к их ведению, а также по выявлению, предупреждению, пресечению и раскрытию деятельности незаконных вооруженных формирований, преступных групп, отдельных лиц и общественных объединений, ставящих своей целью насильственное изменение конституционного строя Российской Федерации.

При осуществлении разведывательной и контрразведывательной деятельности органы ФСБ руководствуются ведомственными нормативными актами, а при организации борьбы с преступностью – ФЗ «Об ОРД».

Федеральные органы государственной охраны осуществляют ОРД в целях обеспечения безопасности высших органов законодательной, исполнительной и судебной властей Российской Федерации и их должностных лиц. Согласно ст.1 ФЗ «О государственной охране» под государственной охраной понимается деятельность по обеспечению безопасности объектов государственной охраны и защите охраняемых объектов, выполняемая в целях безопасного и беспрепятственного осуществления государственной власти в Российской Федерации и исполнения международных обязательств Российской Федерации, осуществляемая на основе совокупности правовых, организационных, охранных, режимных, оперативно-розыскных, технических, информационных и иных мер.

К объектам государственной охраны относятся:

- Президент РФ и члены его семьи, проживающие совместно с ним или сопровождающие его;
- председатель Правительства РФ;
- председатель Совета Федерации Федерального Собрания РФ;
- председатель Государственной Думы Федерального Собрания РФ;
- председатель Конституционного суда РФ;
- председатель Верховного суда РФ;
- председатель Высшего арбитражного суда РФ;

- генеральный прокурор РФ;
- председатель Следственного комитета РФ.

Указанным лицам государственная охрана предоставляется в течение срока их полномочий.

К объектам государственной охраны относятся также главы иностранных государств и правительств и иные лица иностранных государств во время пребывания на территории РФ.

По решению Президента РФ государственная охрана может быть предоставлена иным лицам, замещающим государственные должности РФ, членам Совета Федерации, депутатам Государственной Думы и федеральным государственным служащим.

Таможенные органы, в соответствии со ст. 19 ФЗ «О таможенном регулировании в Российской Федерации», осуществляют ОРД в целях выявления, предупреждения, пресечения и раскрытия преступлений, производство неотложных следственных действий и дознания по которым отнесено уголовно-процессуальным законодательством Российской Федерации к ведению таможенных органов, выявления и установления лиц, их подготавливающих, совершающих или совершивших, а также в целях обеспечения собственной безопасности.

В исправительных учреждениях *ФСИН России* ОРД осуществляется оперативными аппаратами исправительных учреждений, а также другими уполномоченными органами в пределах их компетенции. В соответствии со ст. 84 УИК РФ задачами ОРД являются: обеспечение личной безопасности осужденных, персонала исправительных учреждений и иных лиц; выявление, предупреждение и раскрытие готовящихся и совершаемых в исправительных учреждениях преступлений и нарушений установленного порядка отбывания наказания; розыск в установленном порядке осужденных, совершивших побег из исправительных учреждений, а также осужденных, уклоняющихся от отбывания лишения свободы; содействие в выявлении и раскрытии преступлений, совершенных осужденными до прибытия в исправительное учреждение.

Оперативные подразделения уголовно-исполнительной системы осуществляют ОРД и при исполнении наказаний, не связанных с изоляцией осужденных от общества. В частности, проводят первоначальные розыскные мероприятия в отношении осужденных к наказаниям в виде обязательных работ, исправительных работ, ограничения свободы, а также условно осужденных, осужденных с отсрочкой отбывания наказания, уклоняющихся от контроля уголовно-исполнительных инспекций; объявляют их розыск.

Оперативные подразделения системы МВД России и их задачи

Перечень оперативных подразделений ОВД, осуществляющих ОРД в борьбе с преступностью, определен приказом МВД России от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России». В зависимости от полномочий данные подразделения и службы можно разделить на две группы. Подразделения первой группы осуществляют ОРД в полном объеме и наделены полномочиями по применению всех сил, средств и методов ОРД. Эту группу составляют:

- подразделения уголовного розыска;
- подразделения экономической безопасности и противодействия коррупции;
- подразделения собственной безопасности;
- подразделения по противодействию экстремизму;
- подразделения по борьбе с преступными посягательствами на грузы;
- подразделения по обеспечению безопасности лиц, подлежащих государственной защите;
- оперативно-поисковые подразделения;
- подразделения специальных технических мероприятий (оперативно-технические подразделения) (далее – ПСТМ);
- межрегиональные оперативно-розыскные подразделения территориальных органов МВД России на окружном уровне;
- подразделения по контролю за оборотом наркотиков.

Вторую группу составляют подразделения, осуществляющие ОРД в ограниченном объеме. К ним относятся подразделения по обеспечению взаимодействия с правоохранительными органами иностранных государств – членов Международной организации уголовной полиции – Интерпола и Генеральным секретариатом Интерпола.

Основными задачами *подразделений уголовного розыска* являются выявление, предупреждение, пресечение и раскрытие преступлений, отнесенных к компетенции уголовного розыска; розыск лиц, скрывающихся от органов дознания, следствия и суда, розыск без вести пропавших лиц, установление личности по неопознанным трупам.

В круг задач *подразделений экономической безопасности и противодействия коррупции* входят выявление, предупреждение, пресечение и раскрытие преступлений в сфере экономики, а также против интересов государственной власти, совершаемых в федеральных органах государственной власти; организация и проведение профилактических мероприятий и ОРМ по защите всех форм собственности от

преступных посягательств в целях обеспечения благоприятных условий для развития предпринимательства и инвестиционной деятельности.

Для *подразделений собственной безопасности* основными задачами являются:

- выявление коррумпированных сотрудников в ОВД, а также лиц, замышляющих, подготавливающих или совершающих должностные и иные преступления;
- обеспечение личной безопасности сотрудников ОВД, членов их семей и близких, а также лиц, оказывающих содействие подразделениям, осуществляющим ОРД;
- выявление, предупреждение и пресечение попыток проникновения преступных элементов в систему ОВД или оказания негативного влияния на ее деятельность.

Подразделения по противодействию экстремизму осуществляют предупреждение, выявление и раскрытие преступлений экстремисткой направленности.

Основной задачей *подразделений ОВД на транспорте по борьбе с преступными посягательствами на грузы* является предупреждение, выявление и раскрытие хищений грузов из подвижного состава и складских объектов транспортной инфраструктуры.

Подразделения по обеспечению безопасности лиц, подлежащих государственной защите, применяют меры безопасности в целях защиты жизни и здоровья участников уголовного судопроизводства, подлежащих государственной защите, а также по обеспечению сохранности их имущества.

Основной задачей *оперативно-поисковых подразделений* является получение информации, представляющей оперативный интерес, путем проведения оперативно-поисковых мероприятий с использованием негласных методов и средств.

Назначение *ПСТМ ОВД* состоит в организации и проведении оперативно-технических мероприятий (далее – ОТМ) по заданиям оперативно-розыскных служб, техническом обеспечении ОРМ в целях негласного получения информации и документирования преступной деятельности, а также координации своей деятельности с оперативно-техническими подразделениями ФСБ России.

Оперативно-поисковые подразделения и ПСТМ работают в особом режиме конспирации по заданиям оперативных подразделений ОВД.

Межрегиональные оперативно-разыскные подразделения территориальных органов МВД России на окружном уровне занимаются

координацией деятельности нижестоящих подразделений, а также раскрытием преступлений, имеющих межрегиональный характер.

В задачи *подразделений по контролю за оборотом наркотиков* входят выявление, предупреждение, пресечение и раскрытие преступлений, связанных с незаконным оборотом наркотиков

Основной задачей *подразделений по обеспечению взаимодействия с правоохрнительными органами иностранных государств – членов Международной организации уголовной полиции – Интерпола и Генеральным секретариатом Интерпола* является проведение ОРМ по запросам международных правоохрнительных организаций и правоохрнительных органов иностранных государств.

Должностные лица оперативных подразделений органов внутренних дел, их обязанности и права

Оперативные подразделения ОВД состоят из штатных сотрудников, т. е. лиц, имеющих специальные звания полиции, осуществляющих оперативно-розыскные функции преимущественно легально гласно, и оперативных сотрудников, чья принадлежность к правоохрнительным органам конспирируется (т. е. их работа осуществляется только негласно). Первые вправе сочетать проведение ОРМ с административно-правовыми, уголовно-процессуальными и другими правовыми действиями. Вторые же, к числу которых относятся сотрудники оперативно-технических и оперативно-поисковых подразделений, применяют только разведывательные методы по добыванию информации и скрывают свою принадлежность к органам внутренних дел.

К должностным лицам органов внутренних дел относятся следующие категории оперативных сотрудников:

- младшие оперуполномоченные;
- оперуполномоченные и старшие оперуполномоченные;
- оперуполномоченные и старшие оперуполномоченные по особо важным делам;
- руководители оперативных подразделений.

Для выполнения возложенных задач штатные гласные сотрудники оперативных подразделений ОВД законодательными и ведомственными нормативными актами наделены соответствующей оперативно-розыскной, административно-правовой и уголовно-процессуальной компетенцией.

Оперативно-розыскная компетенция закреплена в ФЗ «Об ОРД», где определены обязанности и права органов, осуществляющих ОРД.

Органы, осуществляющие ОРД, согласно ст. 14 ФЗ «Об ОРД», обязаны:

- принимать в пределах своих полномочий все необходимые меры по защите конституционных прав и свобод человека и гражданина, собственности, а также по обеспечению безопасности общества и государства;

- исполнять в пределах своих полномочий поручения в письменной форме органа дознания, следователя, руководителя следственного органа о проведении ОРМ по уголовным делам и материалам проверки сообщений о преступлении, принятым ими к производству, а также решения суда по уголовным делам;

- выполнять на основе и в порядке, предусмотренных международными договорами Российской Федерации, запросы соответствующих международных правоохранительных организаций, правоохранительных органов и специальных служб иностранных государств;

- информировать другие органы, осуществляющие оперативно-розыскную деятельность на территории Российской Федерации, о ставших им известными фактах противоправной деятельности, относящихся к компетенции этих органов, и оказывать этим органам необходимую помощь;

- соблюдать правила конспирации при осуществлении ОРД;

- содействовать обеспечению в порядке, установленном законодательством Российской Федерации, безопасности и сохранности имущества своих сотрудников, лиц, оказывающих содействия органам, осуществляющим ОРД, участников уголовного судопроизводства, а также членов семей и близких указанных лиц от преступных посягательств.

Для эффективного исполнения своих обязанностей оперативные подразделения ОВД наделены следующими правами (ст. 15 ФЗ «Об ОРД»):

- проводить гласно и негласно ОРМ, производить при их проведении изъятие предметов, материалов и сообщений, а также прерывать предоставление услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации;

- устанавливать на безвозмездной либо возмездной основе отношения сотрудничества с лицами, изъявившими согласие оказывать

содействие на конфиденциальной основе органам, осуществляющим ОРД;

- использовать в ходе проведения ОРМ по договору или устному соглашению служебные помещения, имущество предприятий, учреждений, организаций, воинских частей, а также жилые и нежилые помещения, транспортные средства и иное имущество частных лиц;

- использовать в целях конспирации документы, зашифровывающие личность должностных лиц, ведомственную принадлежность предприятий, учреждений и организаций, подразделений, помещений и транспортных средств органов, осуществляющих ОРД, а также личность граждан, оказывающих им содействие на конфиденциальной основе;

- создавать в установленном законодательством порядке предприятия, учреждения, организации и подразделения, необходимые для решения задач, предусмотренных федеральным законом.

В то же время должностные лица оперативных подразделений ОВД наделены административно-правовой компетенцией, поскольку в соответствии с ФЗ «О полиции» они являются представителями власти и наделены определенными государственно-властными полномочиями, которые применяются в отношении граждан. Так, для решения задач ОРД они вправе:

- проверять документы, удостоверяющие личность граждан, если имеются данные, дающие основания подозревать их в совершении преступлений или полагать, что они находятся в розыске;

- вызывать в полицию граждан и должностных лиц по расследуемым уголовным делам и находящимся в производстве делам об административных правонарушениях;

- в связи с расследуемыми уголовными делами и находящимися в производстве делами об административных правонарушениях получать на безвозмездной основе по мотивированному запросу сведения, справки, документы (их копии), иную необходимую информацию, в том числе персональные данные граждан, за исключением случаев, когда федеральным законом установлен иной порядок получения информации;

- беспрепятственно по предъявлению служебного удостоверения посещать в связи с расследуемыми уголовными делами и находящимися в производстве делами об административных правонарушениях государственные и муниципальные органы, общественные объединения и организации, знакомиться с необходимыми докумен-

тами и материалами, в том числе с персональными данными граждан, имеющими отношение к расследуемым уголовным делам, производству по делам об административных правонарушениях;

- проводить регистрацию, фотографирование, аудио-, кино- и видеосъемку, дактилоскопирование лиц, задержанных по подозрению в совершении преступления, заключенных под стражу обвиняемых в совершении преступлений, подвергнутых административному наказанию в виде административного ареста, иных задержанных лиц, если в течение установленного срока задержания достоверно установить их личность не представляется возможным.

В соответствии с действующим законодательством сотрудники оперативных подразделений органов внутренних дел обладают полномочиями по применению отдельных мер государственного принуждения. К ним относятся: задержание; входжение (проникновение) в жилые и иные помещения, на земельные участки и территории; оцепление (блокирование) участков местности, жилых помещений, строений и других объектов; формирование и ведение банков данных о гражданах. Для предотвращения и пресечения преступлений и административных правонарушений они имеют право на применение физической силы, специальных средств и огнестрельного оружия.

Сотрудники оперативных подразделений ОВД в соответствии со ст. 12 ФЗ «О полиции» должны выполнять следующие обязанности:

- принимать и регистрировать заявления и сообщения о преступлениях, осуществлять проверку заявлений и сообщений о преступлениях и принимать по таким заявлениям и сообщениям меры, предусмотренные законодательством Российской Федерации;

- прибывать незамедлительно на место совершения преступления, пресекать противоправные деяния, устранять угрозы безопасности граждан и общественной безопасности, документировать обстоятельства совершения преступления;

- выявлять причины преступлений и условия, способствующие их совершению, принимать в пределах своих полномочий меры по их устранению; выявлять лиц, намеревающихся совершить преступление, и проводить с ними индивидуальную профилактическую работу; и некоторые другие.

Уголовно-процессуальная компетенция оперативных подразделений ОВД определена УПК РФ, ст. 40 которого отнесла данные подразделения к органам дознания и возложила на них дознание по уголовным делам, по которым производство предварительного следствия необязательно, а также выполнение неотложных следственных дей-

ствий по уголовным делам, по которым производство предварительного следствия обязательно.

Оперативно-розыскная, административно-правовая и уголовно-процессуальная компетенции сотрудника оперативных подразделений конкретизируются его специализацией. Выделяют следующие виды специализаций:

- зональная (территориальная);
- линейная;
- объектово-отраслевая;
- функциональная.

Сущность *зональной специализации* состоит в том, что на сотрудника оперативного подразделения возлагается обязанность по организации и осуществлению ОРД на определенной территории (оперативной зоне).

Линейная специализация подразумевает осуществление ОРД для борьбы с однородными группами преступлений, например, против личности, краж чужого имущества и т. д.

Объектово-отраслевая специализация состоит в том, что ОРД осуществляется для выявления и раскрытия отдельных видов преступлений на предприятиях определенной отрасли или на отдельных крупных объектах. Объектово-отраслевая специализация характерна для подразделений ЭБиПК.

Функциональная специализация выражается в том, что сотрудник оперативного подразделения выполняет одну из функций, отнесенных к компетенции оперативного подразделения, например, розыскную работу.

К сотрудникам оперативных подразделений предъявляются специальные профессиональные, морально-этические, психологические и иные требования.

Оперативные подразделения ОВД и представляющие их сотрудники при решении стоящих перед ними задач руководствуются Конституцией РФ, ФЗ «Об ОРД», другими законами и ведомственными нормативными актами. Они самостоятельно принимают решения о заведении ДОУ и производстве по ним; планируют ОРМ, определяют основания, организацию и тактику их проведения; принимают другие решения и несут за это ответственность. Их деятельность носит публичный характер. При исполнении служебных обязанностей, являясь представителями власти, они находятся под защитой государства.

Примерный план занятия

1. Органы, осуществляющие ОРД, их общая характеристика и специфические функции.
2. Обязанности сотрудников оперативных подразделений и их содержание.
3. Задачи, компетенции и объем полномочий органов и должностных лиц, осуществляющих ОРД.
4. Взаимосвязь прав и обязанностей органов и должностных лиц, осуществляющих ОРД.
5. Оперативные подразделения, уполномоченные на осуществление ОРД в системе МВД России.

Вопросы для самоконтроля по теме

1. Назовите органы, осуществляющие ОРД.
2. Назовите категории оперативных сотрудников.
3. Перечислите оперативные подразделения системы МВД России.
4. Назовите компетенции сотрудников оперативных подразделений.

Тема 2.6. Лица, оказывающие конфиденциальное содействие (сотрудничество) органам внутренних дел

Понятие конфиденциального содействия (сотрудничества) граждан оперативным подразделениям органов внутренних дел

Эффективность служебной деятельности по борьбе с преступностью достигается высокой оперативной осведомленностью, позволяющей противостоять криминальным проявлениям в современном обществе. Чем больше качественной оперативно значимой информации поступает в ОВД, чем выше уровень ее анализа, тем эффективнее прогнозирование и планирование оперативно-служебной деятельности и достовернее статистические показатели¹.

Добиться высоких показателей в предупреждении, выявлении и раскрытии преступлений, совершаемых неочевидно, можно путем осуществления целенаправленной деятельности по привлечению граждан на конфиденциальной основе к участию в ОРМ, а также к добыванию оперативно значимой информации.

Впервые право на установление отношений содействия на законодательном уровне было закреплено в 1992, а затем в 1995 г. в ст. 17 и 18 ФЗ «Об ОРД», обеспечив возможность реализации гражданами своего права на добровольное оказание помощи ОВД в решении задач борьбы с преступностью путем содействия аппаратам ОВД на гласной и негласной основе. В законе признана социальная значимость, полезность и необходимость такого содействия, а ОВД предоставлено право на его установление. Граждане оказывают содействие в подготовке и участии в ОРМ, а также предоставляют оперативно значимую информацию сотрудникам ОВД как на возмездной (в том числе и по контракту), так и на безвозмездной основе.

Содействие представляет собой комплекс организационных мер, проводимых оперативными подразделениями полиции, обусловленных оперативно-розыскным законом и другими подзаконными актами, направленными на привлечение граждан с их добровольного согласия, на возмездной или безвозмездной основе, гласно и негласно к подготовке и проведению ОРМ, а также предоставление ими оперативно значимой информации для решения задач борьбы с преступностью.

¹ Попов В.Л. Теоретико-правовые аспекты проблемы совершенствования оперативно-розыскной деятельности. Калининград: Калининградский юрид. ин-т МВД России, 1998. С. 68.

Сущность, социально-правовые и морально-этические основы конфиденциального содействия (сотрудничества) граждан оперативным подразделениям ОВД, его значение в борьбе с преступностью

В ФЗ «Об ОРД» вопросам конфиденциального содействия граждан посвящена гл. IV «Содействие граждан органам, осуществляющим ОРД», в которой определено понятие содействия, раскрыты условия привлечения граждан к проведению ОРМ, социальная и правовая защита таких лиц. Значимости института содействия посвящены ч. 2 ст. 6, ст. 17 и 18. Тем самым государство осознает необходимость законодательного оформления содействия и противодействует нападкам и гонениям на конфиденентов со стороны отдельных должностных лиц и средств массовой информации. Более того, оно официально закрепило их социальные и правовые гарантии, взяв под свою защиту граждан, оказывающих содействие правоохранительным органам в борьбе с преступностью.

Федеральный закон «Об ОРД» – не единственный законодательный акт, регламентирующий конфиденциальное содействие (сотрудничество) граждан с оперативными аппаратами ОВД. Так, ФЗ «О полиции» в п. 34 ст. 13 указывает, что полиции предоставляются права «привлекать граждан с их согласия к внештатному сотрудничеству; устанавливать негласное сотрудничество с гражданами, изъявившими желание конфиденциально оказывать содействие на безвозмездной или возмездной основе; объявлять о назначении вознаграждения за помощь в раскрытии преступлений и задержании лиц, их совершивших, и выплачивать его гражданам и организациям; поощрять граждан, оказавших помощь полиции в выполнении иных возложенных на нее обязанностей...». Организация и тактика привлечения граждан к содействию (сотрудничеству на конфиденциальной основе) регламентируется закрытыми НПА МВД России.

Значимость института содействия заключается в том, что, благодаря помощи граждан оперативным подразделениям полиции удастся предотвратить ухудшение криминальной ситуации, так как поступающая от граждан информация позволяет прогнозировать обострение оперативной обстановки и незамедлительно реагировать на преступные проявления. Зачастую проверка поступившей от граждан информации намного результативнее проведения ОРМ по нераскрытым преступлениям.

Существенной гарантией защиты прав и законных интересов личности в сфере ОРД является то, что эта деятельность осуществля-

ется не только в отношении граждан, по которым проводятся ОРМ, но и граждан, оказывающих конфиденциальное содействие. Лица, оказывающие содействие оперативным подразделениям полиции, как указано в ст. 18 ФЗ «Об ОРД», находятся под защитой государства, которое им обеспечивает выполнение своих обязательств, предусмотренных контрактом, в том числе гарантирует вознаграждение за свой труд, правовую защиту, связанную с правомерным выполнением указанными лицами общественного долга или возложенных на них обязанностей, социальную и материальную помощь. В этой же статье указано, что сведения о лицах, содействующих правоохранительным органам в борьбе с преступностью, составляют государственную тайну.

При возникновении реальной угрозы противоправного посягательства на жизнь, здоровье или имущество отдельных лиц в связи с их содействием органам, осуществляющим ОРД, а равно членов их семей и близких эти органы обязаны принять необходимые меры по предотвращению противоправных действий, установлению виновных и привлечению их к ответственности, предусмотренной законодательством Российской Федерации.

Лица, сотрудничающие с оперативными подразделениями ОВД, либо оказавшие им помощь в раскрытии преступлений или установлении лиц, их совершивших, могут получать вознаграждения и другие выплаты. Полученные указанными лицами суммы вознаграждений и другие выплаты налогами не облагаются и в декларациях о доходах не указываются.

Граждане, сотрудничающие по контракту с органами, осуществляющими ОРД, в качестве основного рода занятий, имеют право на пенсионное обеспечение в соответствии с законодательством Российской Федерации. Период такого сотрудничества засчитывается в страховой стаж указанных граждан на основании сведений соответствующих органов.

В целях обеспечения безопасности лиц, сотрудничающих с оперативными подразделениями ОВД, и членов их семей допускается проведение специальных мероприятий по их защите в порядке, определяемом законодательными и иными нормативными правовыми актами Российской Федерации.

В случае гибели лица, сотрудничающего по контракту с органами, осуществляющими ОРД, в связи с его участием в проведении ОРМ семье пострадавшего и лицам, находящимся на его иждивении, выплачивается единовременное пособие в размере десятилетнего де-

нежного содержания погибшего и назначается пенсия по случаю потери кормильца.

При получении таким гражданином в связи с его участием в проведении ОРМ травмы, ранения, контузии, увечья, исключающих для него возможность дальнейшего сотрудничества с органами, осуществляющими ОРД, ему выплачивается единовременное пособие в размере пятилетнего денежного содержания и назначается пенсия по инвалидности.

При одновременном возникновении нескольких оснований для указанных единовременных выплат они осуществляются по одному основанию по выбору получателя.

Следует учитывать, что мотивы согласия лица на сотрудничество могут быть различными. Недопустимо получать согласие гражданина на сотрудничество, используя методы, унижающие его честь и достоинство.

Виды и формы содействия (сотрудничества) граждан органам внутренних дел. Основания и порядок привлечения к конфиденциальному содействию (сотрудничеству) и прекращения содействия (сотрудничества)

К содействию на конфиденциальной основе могут привлекаться исключительно отдельные лица. Поскольку этот вид содействия содержит сведения, составляющие государственную тайну, то осуществляется в строгом соответствии с принципом конспирации.

Нормативные правовые акты МВД России предусматривают следующие виды содействия:

- **анонимное содействие**, предполагающее передачу оперативно-значимой информации в оперативные подразделения ОВД непосредственно или посредством средств телекоммуникации лицом, скрывающим свои персональные данные (оперативному сотруднику запрещается выяснять личность анонима);

- **содействие на оперативном контакте**, которое выражается в однократном предоставлении оперативно значимой информации оперативному сотруднику гражданином, который в общении не скрывает своих данных, однако не желает быть участником уголовного судопроизводства;

- **конфиденциальное содействие (сотрудничество)** граждан на долговременной основе с оперативными аппаратами ОВД, которое регламентируется закрытыми НПА МВД России.

Содействие граждан оперативным подразделениям ОВД осуществляется в двух формах – бесконтрактной и контрактной.

Бесконтрактная форма содействия представляет собой, как правило, разовое получение конфиденциальной информации от граждан (это называется оперативным контактом гражданина с оперативным сотрудником).

Контрактная форма содействия предполагает долговременное сотрудничество гражданина на конфиденциальной основе с оперативными подразделениями ОВД. Федеральный закон «Об ОРД» предусматривает добровольное согласие гражданина на оказание содействия на контрактной основе. Порядок заключения контракта на конфиденциальной основе подробно излагается в Наставлении об основах организации и тактики ОРД ОВД Российской Федерации¹.

Общие правила, вытекающие из содержания ст. 17 ФЗ «Об ОРД»:

1) контракт (договор) может заключаться только с совершеннолетним дееспособным лицом (в соответствии со ст. 60 Конституции РФ гражданин может самостоятельно осуществлять в полном объеме свои права и обязанности с 18 лет);

2) контракт должен осуществляться по обоюдному согласию сторон и учитывать специфику отношений конкретного лица с «работодателем»;

3) контракт – это документ, создающий определенные обязанности и права для обеих сторон;

4) контракт считается юридической гарантией для лиц, являющихся сторонами в устанавливаемых отношениях.

Органам, осуществляющим ОРД, запрещено использовать на контрактной основе для подготовки и проведения ОРМ представителей всех уровней законодательной власти, судей, прокуроров, адвокатов, священнослужителей и представителей официально зарегистрированных религиозных объединений. Однако предполагается возможность сотрудничества указанной группы лиц на бесконтрактной основе.

Контракт как разновидность договора имеет правовые последствия для обеих сторон, поэтому он должен отвечать ряду требований. Содержание контракта не должно быть двусмысленным или неясным². В контракте следует определить цель сотрудничества; обязанности и права сторон; срок, на который он заключается, а также условия возможного продления или досрочного расторжения; вид,

¹ Утверждено приказом МВД России от 04.04.2013 № 001.

² Об оперативно-розыскной деятельности: Научно-практический комментарий к федеральному закону / под ред. Н.В. Николука. М., 2002. С. 166.

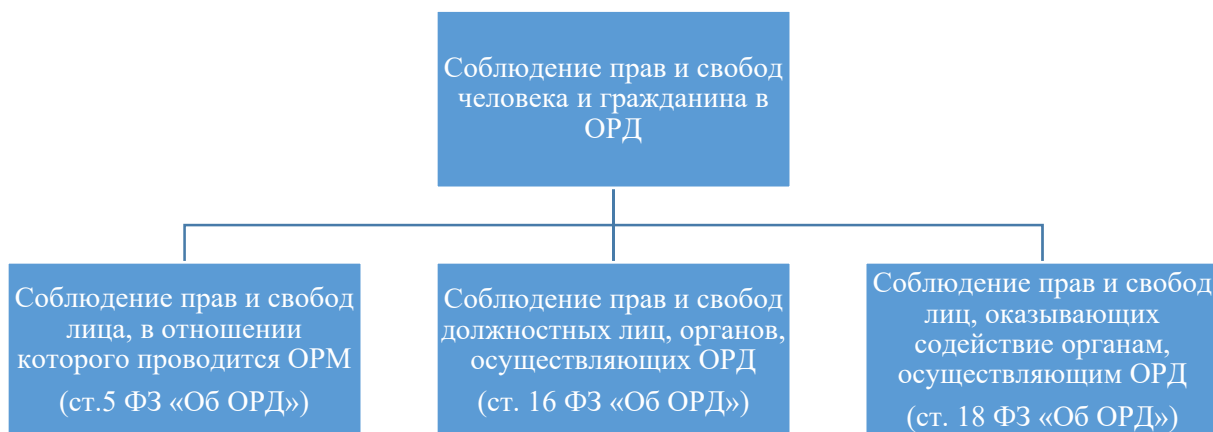
размер и порядок вознаграждения гражданину за проделанную работу, а также обязательства, связанные с обеспечением его личной безопасности, возмещением понесенного в связи с выполнением заданий материального и морального ущерба, социальным обеспечением его и членов его семьи, и другие обязательства в соответствии с действующим гражданским законодательством. В контракте могут оговариваться особые условия выполнения задания.

Действие контракта начинается с момента его подписания. При нарушении гражданином взятых на себя обязательств оперативный сотрудник имеет право внести предложение об изменении оговоренных ранее условий контракта. Гражданин может обжаловать действия органа или указанного сотрудника, связанные с нарушением условий контракта, в установленном законом порядке.

Контракт прекращается по инициативе одной из сторон и при наличии оснований, в частности:

- окончания действия контракта или выполнения условий сотрудничества;
- утраты гражданином возможности оказывать помощь органам, осуществляющим ОРД;
- приобретения гражданином статуса народного депутата, судьи, прокурора, адвоката, священнослужителя или полномочного представителя официально зарегистрированных религиозных объединений;
- уклонения от сотрудничества;
- нарушения условий контракта, других договоренностей о сотрудничестве;
- грубых нарушений требований конспирации;
- умышленного предоставления ложной информации;
- использования конфиденциального сотрудничества для прикрытия своих преступных замыслов.

Инициатор досрочного прекращения контракта уведомляет о своем намерении устно или письменно другую сторону.



Вопросы для самостоятельного изучения

1. Исторический опыт привлечения граждан к конфиденциальному содействию правоохрнительным органам в России.
2. Понятие дееспособности лица, оказывающего конфиденциальное содействие оперативным подразделениям ОВД.

Примерный план занятия

1. Понятие конфиденциального содействия (сотрудничества) граждан оперативным подразделениям органов внутренних дел.
2. Сущность, социально-правовые и морально-этические основы конфиденциального содействия (сотрудничества) граждан оперативным подразделениям ОВД, его значение в борьбе с преступностью.
3. Виды и формы содействия (сотрудничества) граждан органам внутренних дел. Основания и порядок привлечения к конфиденциальному содействию (сотрудничеству) и прекращения содействия (сотрудничества).

Вопросы для самоконтроля по теме

1. Назовите цели в оперативно-розыскной деятельности, решаемые посредством привлечения граждан к содействию.
2. Какие нормативные правовые акты законодательного и подзаконного уровня регламентируют вопросы привлечения граждан к содействию?
3. Назовите виды конфиденциального содействия и его отличие от сотрудничества.
4. Каких лиц запрещено законом использовать на контрактной основе для подготовки и проведения ОРМ органом, осуществляющим ОРД?

Тема 2.7. Оперативно-розыскные мероприятия и их характеристика

Оперативно-розыскные мероприятия представляют собой один из основных источников оперативно-розыскной информации. Перечень ОРМ содержится в ст. 6 ФЗ «Об ОРД». Под ОРМ принято понимать предусмотренные законом действия преимущественно конспиративного характера, осуществляемые должностными лицами оперативных подразделений в целях получения и проверки оперативной информации об обстоятельствах, имеющих значение для предупреждения и раскрытия преступлений, осуществления розыскной работы, а также решения иных задач ОРД.

Оперативно-розыскные мероприятия могут проводиться исключительно должностными лицами оперативных подразделений в целях получения и проверки оперативной информации об обстоятельствах, представляющих оперативный интерес. К участию в ОРМ могут привлекаться иные субъекты ОРД. Так, применение при проведении ОРМ криминалистической техники требует помощи специалистов – сотрудников экспертно-криминалистических подразделений. К участию в ОРМ могут привлекаться и иные специалисты: сотрудники контрольно-ревизионных органов, санитарно-эпидемиологических, экологических и иных организаций и учреждений, частные лица.

Особое место в проведении ОРМ занимают лица, оказывающие содействие оперативным подразделениям ОВД на конфиденциальной основе. Выполняя задания по получению или проверке оперативной информации, такие лица в своей деятельности невольно обращаются к возможностям тех или иных ОРМ (опросы, осмотры, наблюдение и т. п.). Однако организатором подобных ОРМ во всех случаях выступает оперативный сотрудник, определяющий необходимость проведения ОРМ исходя из стоящих перед ним задач, он же несет ответственность за их результаты. Давая определенное задание, оперативный сотрудник обязан инструктировать соответствующих лиц о том, какие тактические приемы следует использовать в целях получения нужной информации, какую и каким образом оперативную технику применять.

Субъектом ОРМ во всех случаях является сам оперативный сотрудник. Он же, как правило, осуществляет документальное оформление хода и результатов проводимых ОРМ. Иные привлекаемые к их проведению лица являются лишь участниками ОРМ.

В соответствии со ст. 6 ФЗ «Об ОРД» при осуществлении ОРД проводятся следующие ОРМ:

- 1) опрос;
- 2) наведение справок;
- 3) сбор образцов для сравнительного исследования;
- 4) проверочная закупка;
- 5) исследование предметов и документов;
- 6) наблюдение;
- 7) отождествление личности;
- 8) обследование помещений, зданий, сооружений, участков местности и транспортных средств;
- 9) контроль почтовых отправлений, телеграфных и иных сообщений;
- 10) прослушивание телефонных переговоров;
- 11) снятие информации с технических каналов связи;
- 12) оперативное внедрение;
- 13) контролируемая поставка;
- 14) оперативный эксперимент;
- 15) получение компьютерной информации.

Перечень ОРМ может быть изменен или дополнен только федеральным законом.

В специальной литературе предлагается несколько классификаций ОРМ:

- в зависимости от времени (продолжительности) проведения ОРМ – *разовые* и *длящиеся*;
- в зависимости от формы проведения – *гласные* и *негласные*;
- в зависимости от необходимости санкционирования ОРМ – *не требующие какого-либо санкционирования* (опрос, наведение справок, сбор образцов для сравнительного исследования, проверочная закупка и др.), *требующие ведомственного санкционирования* (проверочная закупка и контрольная поставка предметов, веществ и продукции, свободная реализация которых запрещена либо оборот которых ограничен; оперативное внедрение; оперативный эксперимент и др.) и *требующие судебного решения* (контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических каналов связи и др.).

Примерный план занятия

1. Понятие ОРМ. Виды и классификация ОРМ.
2. Оперативно-розыскные мероприятия, осуществляемые по инициативе сотрудников оперативных подразделений, порядок их проведения.
3. Оперативно-розыскные мероприятия, проводимые по постановлению с разрешения руководителя органа, осуществляющего ОРД, порядок их проведения.
4. Оперативно-розыскные мероприятия, осуществляемые по судебному решению, порядок их проведения.

Вопросы для самоконтроля

1. Дайте определение ОРМ.
2. Кто является субъектом ОРМ?
3. Кто может привлекаться к проведению ОРМ?
4. Какие виды ОРМ вам известны?
5. По каким признакам и как могут классифицироваться ОРМ?
6. Для проведения каких ОРМ необходимо судебное решение?
7. Для проведения каких ОРМ достаточно санкции должностных лиц ОВД?
8. Какие ОРМ могут проводиться оперативным сотрудником самостоятельно, без санкций?

Тема 2.8. Оперативно-розыскные мероприятия, ограничивающие конституционные права граждан

Контроль почтовых отправлений, телеграфных и иных сообщений (далее – КПО) – это ОТМ, заключающееся в получении информации о преступной деятельности подозреваемых лиц путем негласного просмотра почтовых отправлений, телеграфных и иных сообщений.

Субъектами КПО, согласно Указу Президента РФ от 1 сентября 1995 г. № 891, могут быть только органы ФСБ.

Объектами КПО могут выступать письма, телеграммы, посылки, бандероли, денежные переводы и иная корреспонденция, в том числе в формате электронных документов и файлов текстовых сообщений, передаваемая по сетям почтовой связи. Контролю может подвергаться корреспонденция, адресованная конкретному лицу или исходящая от него, а также вся корреспонденция, поступающая в конкретный адрес или исходящая из него.

Целью КПО является получение информации, содержащейся в почтовых отправлениях, о преступной деятельности проверяемого лица, его криминальных связях, местонахождении разыскиваемого.

Содержание ОРМ состоит в отборе контролируемых отправлений, их вскрытии, ознакомлении с содержанием и их оценке, снятии копий или фиксации иным способом оперативно значимой информации, в повторной упаковке (при необходимости) и отправлении в адрес. При необходимости с почтовых отправлений снимаются копии, фотографируется содержимое посылок, отбираются образцы для исследования. Материальные носители информации, полученные в результате проведения данного мероприятия, на основании постановления руководителя ОВД и с согласия исполнителя могут быть переданы лицу, в чьем производстве находится уголовное дело, для использования в процессе доказывания.

Порядок проведения ОТМ, связанных с КПО, телеграфных и иных сообщений, и оформления их результатов регламентируется специальными межведомственными и ведомственными нормативными актами.

Организационное обеспечение данного ОРМ включает в себя вынесение постановления руководителем правоохранительного органа с ходатайством о разрешении на установление контроля почтовых отправлений, получение судебного решения по этому вопросу и подготовку задания на его проведение, которое направляется исполните-

лю. Важным элементом организации КПО является установление взаимодействия с предприятиями почтовой связи, законодательной основой которого является Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»¹. В соответствии с законом предприятия связи и операторы связи, действующие на территории РФ, обязаны предоставлять органам, осуществляющим ОРД, возможность проведения ОРМ на сетях связи, принимать меры к недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

Максимальный срок КПО не может превышать шести месяцев и указывается в судебном постановлении. При необходимости продления контроля судья принимает об этом отдельное решение на основании вновь представленных материалов.

В соответствии со ст. 48 Федерального закона от 8 января 1998 г. №3-ФЗ «О наркотических средствах и психотропных веществах» для контроля за хранением, перевозкой или пересылкой наркотических средств, психотропных веществ и их прекурсоров в пределах территорий, на которых решениями компетентных органов власти установлен такой контроль, правоохранительные органы наделены правом производства досмотра почтовых и багажных отправок при наличии достаточных оснований полагать, что осуществляются незаконные операции с наркотиками. Такой досмотр не является ОРМ и не требует судебного решения.

Контроль почтовых отправок имеет сходство с такими следственными действиями, как арест и выемка почтово-телеграфной корреспонденции, однако характеризуется следующими отличиями:

- наложение ареста на почтово-телеграфную корреспонденцию заключается в запрещении доставлять ее адресату без разрешения следователя, т. е. почтовая связь между объектами прерывается;
- исполнение постановления об аресте поручается сотрудникам почтового ведомства, а не оперативно-техническим подразделениям ФСБ России;
- задержанная почтово-телеграфная корреспонденция подвергается осмотру непосредственно следователем, вынесшим постановление о ее аресте, в присутствии понятых.

Контроль почтовых отправок следует отличать от контролируемой поставки предметов, отправляемых по почте. Контроль почтовых отправок носит длящийся характер, а контролируемая по-

¹ О внесении изменений в статьи 46 и 51.1 Федерального закона «О связи»: федер. закон от 30.12.2021 № 465-ФЗ.

ставка распространяется на конкретную посылку и носит разовый характер. Кроме того, их отличают цели и субъекты проведения.

Цензура корреспонденции осужденных и лиц, содержащихся под стражей, досмотр посылок, передач и бандеролей в учреждениях по исполнению наказаний не являются ОРМ. Порядок их осуществления регламентируется уголовно-исполнительным законодательством Российской Федерации.

Прослушивание телефонных переговоров (далее – ПТП) – это ОРМ, заключающееся в негласном контроле, аудиозаписи и прослушивании переговоров проверяемых лиц, ведущихся по телефонным линиям связи.

Целью ОРМ является получение информации о преступной деятельности проверяемых лиц, содержащейся в телефонных разговорах, а также установление их криминальных связей.

Объектом ПТП являются телефонные переговоры лиц, подозреваемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях.

Субъектами данного ОРМ являются оперативно-технические подразделения ОВД, ФСБ. Прослушивание телефонных переговоров по заявлению граждан может проводиться непосредственно сотрудником оперативного подразделения с привлечением при необходимости технических специалистов.

Содержание ОРМ состоит в подключении аппаратуры прослушивания к линиям телефонной связи, электронной записи ведущихся переговоров на автоматические записывающие устройства, последующем прослушивании полученной фонограммы с отражением содержания переговоров в письменном виде.

Срок проведения ПТП не может превышать шести месяцев со дня принятия судебного решения. При необходимости его продления судья выносит дополнительное решение на основании вновь представленных материалов.

К телефонным переговорам следует относить передачу информации путем речевого общения, осуществляемого в непрерывном режиме между двумя или более собеседниками с помощью средств электросвязи, а также одностороннюю передачу речевой информации одного абонента на автоматическое записывающее устройство другого.

Телефонные переговоры, в зависимости от месторасположения абонентов, могут быть местными (в пределах одного административного района, города), междугородними и международными.

К телефонным линиям связи относятся:

- любые сети электросвязи общего пользования, предоставляющие соответствующие услуги населению;
- ведомственные сети связи, имеющие выход на сети связи общего пользования;
- выделенные сети связи непроизводственного назначения;
- сети подвижной радиотелефонной связи;
- системы глобальной подвижной персональной спутниковой связи.

Абонентами телефонной связи являются граждане и организации, с которыми заключен договор об оказании услуг телефонной связи с выделением абонентского номера.

По своему содержанию данное ОРМ аналогично следственному действию, предусмотренному ст. 186 УПК РФ, – контролю и записи переговоров, поэтому по возбужденным уголовным делам целесообразно использовать уголовно-процессуальную форму.

В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц, по их заявлению или с их согласия в письменной форме разрешается прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего ОРД, с обязательным уведомлением соответствующего судьи в течение 48 часов. О возникновении такой угрозы может быть известно от них самих либо из других источников, в том числе конфиденциальных. В заявлении или письменном согласии гражданина должно быть указано, на какой срок он разрешает поставить свой телефон на прослушивание и согласны ли на это проживающие с ним совершеннолетние члены семьи.

При прослушивании телефонных переговоров по заявлению граждан звукозаписывающая аппаратура может включаться только при вызове абонента для фиксации поступающих в его адрес угроз.

Организационное обеспечение ПТП включает в себя подготовку необходимых юридических документов. Для принятия судьей соответствующего решения выносятся мотивированное постановление руководителя правоохранительного органа. В постановлении на проведение ПТП указываются персональные данные контролируемого

объекта, абонентский номер его телефона, а также предполагаемое использование результатов прослушивания в доказывании по уголовным делам. По требованию судьи ему могут предоставляться материалы, подтверждающие обоснованность данного ОРМ. После получения судебного решения инициатор ОРМ составляет задание на его выполнение для подразделения ОТМ.

Если телефонным аппаратом кроме проверяемого лица пользуются другие граждане, не являющиеся объектом контроля, то инициатор ПТП указывает в задании необходимые данные, на основании которых осуществляется отбор информации, относящейся к проверяемому лицу, а информация о других лицах уничтожается.

Обязательным элементом организации ПТП является использование специальных технических средств и аппаратуры аудиозаписи.

Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами. При возбуждении уголовного дела в отношении лица, телефонные и иные переговоры которого прослушиваются, фонограммы записи контролируемых переговоров направляются следователю для приобщения к уголовному делу в качестве вещественных доказательств по постановлению, утвержденному руководителем правоохранительного органа.

Фонограммы и другие материалы, полученные в результате прослушивания телефонных и иных переговоров лиц, в отношении которых не было возбуждено уголовное дело, подлежат уничтожению в течение шести месяцев с момента прекращения прослушивания, о чем должен быть составлен соответствующий протокол.

Снятие информации с технических каналов связи – это ОТМ, заключающееся в контроле и перехвате с помощью специальных средств текстовой, графической и иной информации, передаваемой проверяемыми лицами по техническим каналам связи.

Целью мероприятия является получение информации о преступной деятельности проверяемых лиц, содержащейся в передаваемых по техническим каналам связи сообщениях, а также установление их криминальных связей.

Объектом данного ОРМ является содержание информации, передаваемой проверяемыми лицами по техническим каналам связи, а также сведения о проводимых сеансах связи.

Субъекты ОРМ – оперативно-технические подразделения ОВД, ФСБ. В отдельных случаях снятие информации может проводиться

непосредственно сотрудником оперативного подразделения с привлечением при необходимости технических специалистов.

Содержание ОРМ состоит в подключении специальной аппаратуры к техническим каналам связи, фиксации на электронные носители передаваемых электромагнитных сигналов и последующем декодировании и расшифровке полученной информации.

В ведомственных нормативных актах к техническим каналам отнесены телексные, факсимильные, селекторные, радиорелейные каналы передачи данных, системы персонального радиовызова (пейджинговая связь), а также линии абонентского телеграфирования, IP-телефонии, электронной почты и иных каналов связи.

Порядок снятия информации с технических каналов связи и оформление его результатов регламентируются отдельными межведомственными, ведомственными нормативными актами.

Организационное и техническое обеспечение мероприятия во многом аналогично проведению ПТП, поскольку линии телефонной связи, помимо передачи речевой информации, используются, как правило, для передачи факсимильных сообщений, цифровых данных, межкомпьютерного обмена, видеосигналов и иных сообщений. Для этого к телефонным линиям пользователи подключают как традиционные телефонные аппараты, так и обширный спектр другой электронной аппаратуры (факсы, модемы, компьютеры, охранные устройства сигнализации и др.). В этих условиях принципиальное отличие ПТП от снятия информации состоит в том, что в первом случае контролируется и фиксируется только речевая информация. Контроль же всех остальных форм передачи сведений (графических, текстовых, видеоизображений и иных) должен быть отнесен к снятию информации с технических каналов связи.

Для осуществления данного мероприятия, в отличие от ПТП, используется более сложная электронная аппаратура из-за необходимости съема и преобразования (дешифровки) иных по своей физической природе сигналов.

Электронные носители информации, полученной в результате проведения этого мероприятия, могут быть представлены следователю для использования в процессе доказывания при условии неразглашения сведений, составляющих государственную тайну.

Получение компьютерной информации (далее – ПКИ) – это ОРМ, заключающееся в использовании технических средств и инфор-

мационных технологий для исследования компьютерных систем с целью обнаружения и документирования материальных следов, свидетельствующих о подготовке или совершении преступлений, которые могут содержаться в компьютерных системах в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Содержание данного ОРМ составляют достаточно сложные в техническом плане и требующие специальной подготовки действия, направленные на добывание хранящейся в компьютерных системах или передаваемой по каналам связи информации о лицах, событиях и фактах, вызывающих оперативный интерес.

Основная задача при ПКИ связана с получением копии компьютерной информации, находящейся на машинных носителях информации целевой компьютерной системы.

Получение компьютерной информации требует привлечения специалистов, а ч. 4 ст. 6 ФЗ «Об ОРД» предписывает использование оперативно-технических сил и средств органов ФСБ, ОВД в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими ОРД.

Компьютерная информация – информация в цифровой форме, доступной восприятию ЭВМ, находящаяся в памяти компьютера, на машинных или иных носителях или передающаяся по каналам связи¹.

Компьютерные системы² – совокупность устройств, основанных на использовании программно-вычислительных систем, предназначенных для автоматизированной обработки цифровых данных (персональные компьютеры и сетевые компьютерные устройства, серверы, ноутбуки, сотовые телефоны, смартфоны, планшеты, банкоматы и др.).

Обработка информации в компьютерных системах – выполняемые по заданным в программном обеспечении (ПО) алгоритмам операции по вводу-выводу, передаче, хранению, копированию, модификации и удалению цифровых данных.

Носители компьютерной информации, на которых она может долговременно храниться и с которых может быть перенесена в компьютер при их подключении к нему, – это встроенные и внешние

¹ О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федер. закон от 01.10.2008 № 164-ФЗ.

² Компьютерная система – это набор аппаратных средств и периферийных устройств, составляющих в совокупности вычислительную машину (справочник технического переводчика). URL: https://technical_translator_dictionary.academic.ru/93704

накопители на жестких магнитных дисках и твердотельных дисках (SSD), флэш-карты, оптические диски, CD, DVD и др. Компьютерная информация непродолжительное время может находиться в микросхемах памяти самого компьютера (ОЗУ, ПЗУ, ППЗУ), а также в микросхемах памяти управляемых компьютером периферийных устройств (принтеров, сканеров, факсов и др.). Информация может передаваться между компьютерными устройствами по сетям и каналам связи, подвергаясь обработке в обеспечивающих процесс передачи промежуточных сетевых устройствах (интерфейсах, серверах, маршрутизаторах, концентраторах, модемах и др.), и оставляя в них следы обработки.

Совершенствование устройств и технологий хранения цифровой информации создает предпосылки для размещения в различных файловых хранилищах, локальных компьютерных сетях и обособленных компьютерных системах огромных массивов сведений и их обработки, что обеспечивает для ОРД повышение эффективности информационного поиска.

Получение компьютерной информации, в отличие от схожих ОРМ, часть из которых допускает получение результатов в виде компьютерных файлов (снятие информации с технических каналов связи, наведение справок, сбор образцов для сравнительного исследования и др.), отражает не способ получения оперативно-розыскной информации, а форму, в которой эта информация представлена. Независимость электрических сигналов от средств хранения, обработки и передачи отмечена в примечаниях к ст. 272 УК РФ¹, что дает основания для проведения ОРМ «получение компьютерной информации» в отношении любых компонентов исследуемой компьютерной системы (например, роутера, TV-бокса или смартфона при установлении их принадлежности к домашней сети Wi-Fi).

Получение компьютерной информации может осуществляться:

- 1) при доступе (непосредственном или дистанционном через компьютерную сеть) к устройствам памяти, установленным в компьютере и периферийном оборудовании;
- 2) при копировании данных с внешних устройств хранения информации;

¹ Согласно примечанию к ст. 272 УК РФ «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

3) при получении информации из технических каналов связи и входящих в них промежуточных обслуживающих устройств.

Во всех случаях информация может быть получена в виде отдельных текстовых, графических, аудио- и видеодокументов либо выборок по заданным условиям из специализированных баз данных (файлы и распечатки).

Для определения конкретных действий, способных обеспечить ПККИ, можно выделить возможные источники оперативно значимых компьютерных данных. Условно эти источники могут быть разделены на виды, для каждого из которых имеется своя специфика получения компьютерных данных:

- 1) технические источники оперативно значимой информации;
- 2) информационные ресурсы сети Интернет;
- 3) сетевые каналы коммуникации;
- 4) базы данных, формируемые в информационных системах государственных органов и коммерческих структур, в том числе банков и операторов связи.

Технические источники оперативно значимой информации включают в себя:

- СВТ, включая средства сотовой связи и мобильные устройства, обеспечивающие доступ к сетевым ресурсам, содержащие сведения о разрабатываемых лицах;
- носители компьютерной информации, на которых могут храниться данные, представляющие оперативный интерес;
- устройства, фиксирующие компьютерные данные, поступающие от различных датчиков (радиочастотных идентификаторов, GPS-трекеров, нательных датчиков, передающих физиологические показатели и сведения о местоположении, и т. п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации;
- сетевое оборудование, через которое осуществляются коммуникационные акты разрабатываемых лиц.

Информационные ресурсы сети Интернет как источники ПККИ – это:

- информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих (сайты криминальных структур, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту, ведется про-

паганда криминального образа жизни, вовлекаются в противоправную деятельность новые участники и т. п.);

– места сетевого общения (закрытые сайты, сетевые форумы и чаты, сообщества в социальных сетях и др.) криминально настроенных лиц и их персональные страницы в социальных сетях.

Противоправная деятельность может обнаруживаться в сети Интернет по информационным следам в виде ссылок на материалы, запрещенные к распространению, сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений.

Среди источников получения компьютерной информации особый интерес представляют сетевые каналы коммуникации, задействованные преступниками для координации действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров и т. п. Обнаружение и контроль таких каналов оперативными подразделениями обеспечивает им существенные преимущества. Важно учитывать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через Интернет, постоянно увеличивается (ICQ, Skype, WhatsApp, Viber, Telegramm и др.), причем многие из них представляют услуги шифрования передаваемых данных.

Оперативно значимая информация может быть получена и из таких источников, как выборки, генерируемые по заданным условиям при анализе сведений из различных баз данных, формируемых в информационных системах государственных органов и коммерческих структур, в том числе банков и операторов связи.

Оперативно-розыскное мероприятие «получение компьютерной информации» обеспечивается применением особых способов доступа к информационным источникам. К таким способам могут быть отнесены следующие:

1. Негласное применение специального ПО и оборудования для скрытого съема данных с компьютерных устройств, включая негласный дистанционный доступ к компьютерным устройствам, имеющим сетевое подключение.

2. Оперативно-розыскной мониторинг сетевых информационных ресурсов, реализуемый через автоматизированный поиск источников, содержащих запрещенную к распространению информацию; оперативно-розыскное изучение материалов выявленных источников, связанных с деятельностью преступных сообществ; наблюдение за

закрытыми для общего доступа местами сетевого общения криминальной направленности.

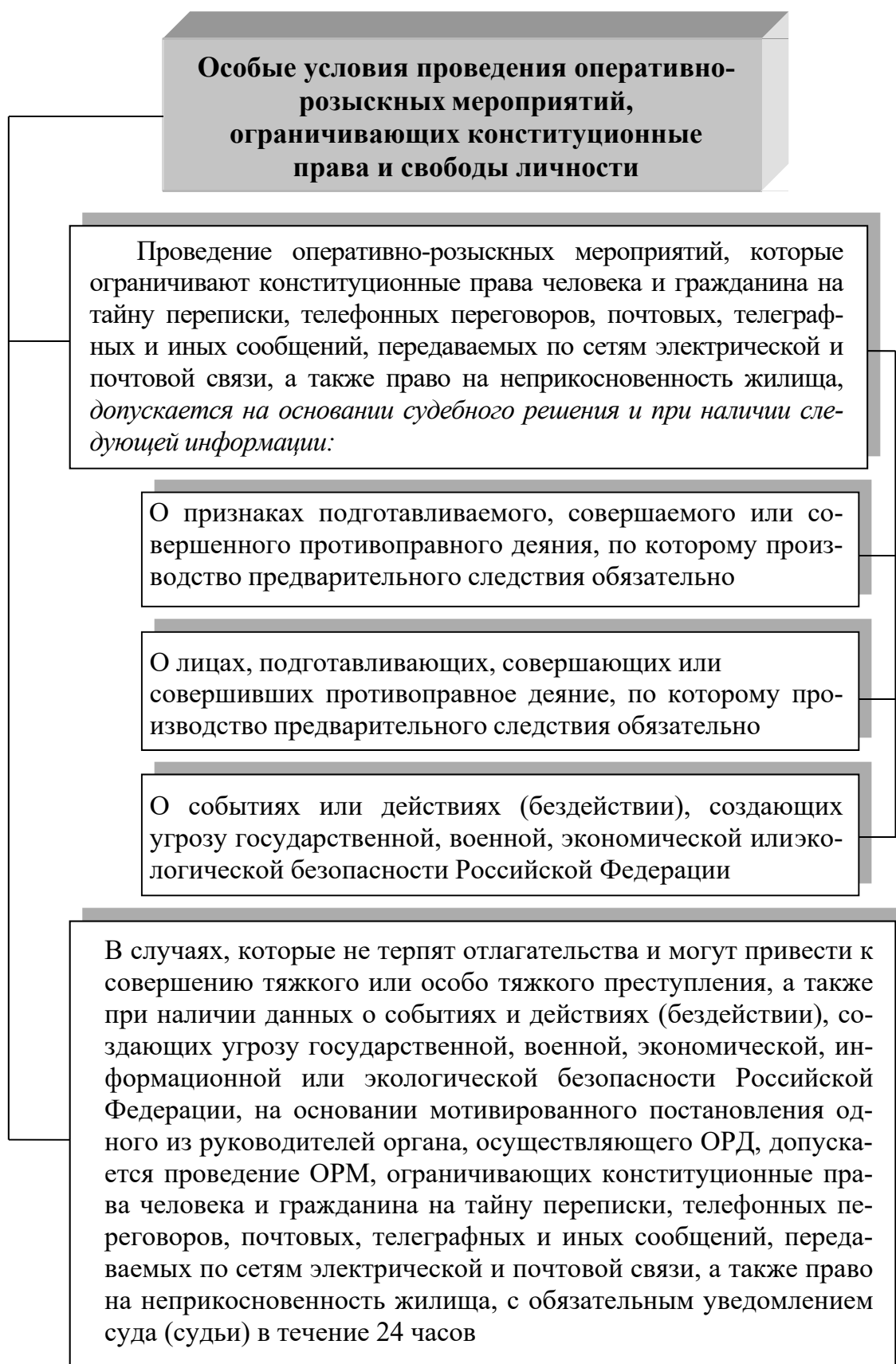
3. Негласная установка в компьютерные устройства разрабатываемых лиц специального ПО, позволяющего фиксировать содержание осуществляемых с этих компьютеров сеансов связи. Формирование файлов с информацией о содержании таких сеансов связи, скрытно направляемых на определенный сетевой адрес, происходит на обозначенном компьютере, в отличие от ОРМ «снятие информации с технических каналов связи», где информация снимается с каналов связи в процессе ее передачи с использованием предоставляемой оператором связи возможности подключения к указанным каналам.

4. Применение аналитического ПО для выявления оперативно значимой информации в базах данных различного назначения. Данный способ получения доступа к информационным источникам соответствует ст. 2 Федерального закона от 6 июля 2016 г. №374-ФЗ, которая дополнила ст. 15 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О ФСБ» частью четвертой, закрепившей право федерального органа исполнительной власти в области обеспечения безопасности получать на безвозмездной основе от государственных органов и государственных внебюджетных фондов необходимые для выполнения возложенных на него обязанностей информационные системы и (или) базы данных, в том числе путем получения возможности удаленного доступа к ним.

5. Негласный или гласный осмотр компьютеров, мобильных телефонов, планшетов и других устройств, при котором хранение данных сопровождается копированием компьютерной информации.

В соответствии с ч. 2 ст. 8 ФЗ «Об ОРД» получение компьютерной информации отнесено к ОРМ, ограничивающих конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, и его проведение допускается на основании судебного решения и при наличии информации, перечисленной в пп. 1–3 данной части ст. 8 ФЗ «Об ОРД». Той же статьей допускается возможность осуществлять получение компьютерной информации без судебного решения по основаниям, предусмотренным п. 5 ч. 2 ст. 7 закона «Об ОРД».

Особые условия проведения оперативно-розыскных мероприятий, ограничивающих конституционные права и свободы личности



Примерный план занятия

1. Виды и характеристика ОРМ, ограничивающих конституционные права граждан.
2. Особенности подготовки и порядок проведения ОРМ, ограничивающих конституционные права граждан.
3. Документальное оформление результатов ОРМ, ограничивающих конституционные права граждан, их использование и хранение.

Вопросы для самоконтроля по теме

1. Кто может проводить контроль почтовых отправлений, телеграфных и иных сообщений?
2. Кому могут быть предоставлены электронные носители информации, полученные в результате проведения ОРМ «снятие информации с технических каналов связи»?
3. Назовите особые условия проведения ОРМ, ограничивающих конституционные права и свободы граждан.
4. Укажите срок проведения ПТП.

Тема 2.9. Основания и условия проведения оперативно-розыскных мероприятий

Для принятия решения о производстве ОРМ должны быть повод и основания.

Поводом могут являться поступившие к оперативному сотруднику сведения о признаках противоправного деяния (события, процесса, явления), которые входят в сферу оперативно-розыскных отношений. Сведения могут поступать в письменной (оперативно-служебные документы, публикации в СМИ, материалы проверок, сообщения конфиденциальных сотрудников и др.) и устной (в случае необходимости быстрого реагирования на развитие криминогенной ситуации) форме.

Основаниями для проведения ОРМ являются фактические данные о непосредственных признаках противоправности деяния или угрозы общественной безопасности, требующие реагирования оперативно-розыскных органов.

В ст. 7 ФЗ «Об ОРД» закреплён перечень оснований проведения ОРМ, наличие которых является важнейшей гарантией соблюдения законности и прав граждан при их осуществлении. Результаты только тех ОРМ, которые были проведены при наличии установленных в законе оснований, могут быть признаны допустимыми доказательствами в суде.

Основания проведения ОРМ могут быть разделены на две основные группы:

1) общие основания, наличие которых позволяет проводить ОРМ, непосредственно направленные на выявление, предупреждение, пресечение и раскрытие преступлений, розыск лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, и лиц, пропавших без вести, а также на решение иных задач по борьбе с преступностью (ч. 1 ст. 7 ФЗ «Об ОРД»);

2) частные основания, выполняющие обеспечивающую функцию, наличие которых позволяет проводить ОРМ, направленные на сбор данных, необходимых для принятия решения о допуске отдельных лиц к определенным сведениям и некоторым видам деятельности, о достоверности представленной ими информации, а также по обеспечению собственной безопасности оперативно-розыскных органов и выполнению возложенных на них задач (ч. 2 и 3 ст. 7 ФЗ «Об ОРД»).



Основания для проведения ОРМ, направленных на собирание данных, необходимых для принятия решений	
О допуске к сведениям, составляющим государственную тайну	
О допуске к работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья людей, а также для окружающей среды	
О допуске к участию в оперативно-розыскной деятельности или о доступе к материалам, полученным в результате ее осуществления	
Об установлении или о поддержании с лицом отношений сотрудничества при подготовке и проведении ОРМ	
По обеспечению безопасности органов, осуществляющих оперативно-розыскную деятельность	
О выдаче разрешений на частную детективную и охранную деятельность	

Условия проведения ОРМ – это предусмотренные законом специальные правила, соблюдение которых обуславливает подготовку и проведение конкретного ОРМ, а также обеспечение реализации принципов оперативно-розыскной деятельности при его проведении	
Общие условия проведения ОРМ	Гражданство, национальность, пол, место жительства, имущественное, должностное и социальное положение, принадлежность к общественным объединениям, отношение к религии и политические убеждения отдельных лиц не являются препятствием для проведения в отношении них ОРМ
	Проводятся на территории Российской Федерации (если иное не предусмотрено Федеральным законом)
Особые условия проведения отдельных ОРМ	

Особые условия проведения ОРМ, ограничивающих конституционные права и свободы человека и гражданина	
Проведение ОРМ, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации	О признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно
	О лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно

	О событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации
В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого или особо тяжкого преступления, а также при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности РФ, на основании мотивированного постановления одного из руководителей органа, осуществляющего ОРД, допускается проведение ОРМ, ограничивающих конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, с обязательным уведомлением суда (судьи) в течение 24 часов	

Особые условия проведения отдельных ОРМ	
Прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях	
Проверочная закупка или контролируемая поставка предметов, веществ и продукции, свободная реализация которых запрещена либо оборот которых ограничен, а также оперативный эксперимент или оперативное внедрение должностных лиц органов, осуществляющих ОРД, а равно лиц, оказывающих им содействие, проводятся на основании постановления, утвержденного руководителем органа, осуществляющего ОРД	
Проведение оперативного эксперимента допускается только в целях выявления, предупреждения, пресечения и раскрытия преступления средней тяжести, тяжкого или особо тяжкого преступления, а также в целях выявления и установления лиц, их подготавливающих, совершающих или совершивших	

Примерный план занятия

1. Сущность правовых оснований проведения ОРМ, определенных Законом «Об ОРД».
2. Условия проведения ОРМ.
3. Правовые основания и условия проведения ОРМ, ограничивающих конституционные права граждан.

4. Особенности проведения ОРМ, ограничивающих конституционные права граждан, в случаях, не терпящих отлагательства.

5. Рассмотрение материалов об ограничении прав граждан при проведении ОРМ как особый вид судебной деятельности.

6. Порядок судебного рассмотрения материалов об ограничении конституционных прав граждан при проведении ОРМ.

Вопросы для самоконтроля по теме

1. Назовите общие основания, наличие которых позволяет проводить ОРМ, непосредственно направленные на решение задач ОРД.

2. Назовите основания, наличие которых позволяет проводить ОРМ, направленные на сбор сведений, необходимых для принятия решения.

3. Назовите общие условия проведения ОРМ.

Тема 2.10. Информационное обеспечение оперативно-розыскной деятельности

Информационное обеспечение – деятельность, направленная на подготовку и доведение информации до ее потребителей.

Специфика информационного обеспечения в конкретной области применения заключается в том, что информация собирается, обрабатывается и представляется в определенной форме. Процесс подготовки информации направлен на создание информационных ресурсов, которые являются необходимым компонентом доведения до потребителя необходимых ему сведений с помощью информационных средств.

Информационное обеспечение ОРД – это деятельность подразделений и служб (оперативных и неоперативных) органов, полномочных осуществлять ОРД, направленная на получение из негласных и гласных источников оперативно значимых данных и их ведение (т. е. сбор, обработка, хранение, передача) в целях решения задач, стоящих перед оперативно-розыскным органом.

Цели информационного обеспечения ОРД:

- а) накопление сведений для раскрытия и предупреждения преступлений;
- б) создание условий для идентификации объектов по их материально-фиксированным отображениям или мысленным образам;
- в) содействие розыску похищенных предметов, а также лиц, как потерпевших, так и совершивших преступление, но скрывшихся от следствия и суда.

Согласно ст. 10 ФЗ «Об ОРД» содержание информационного обеспечения образует деятельность уполномоченных на то законом лиц по созданию и использованию информационных систем, заведению ДООУ с целью систематизации собранных сведений, проверки и оценки результатов ОРД, а также принятия на их основе соответствующих решений.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

В теории ОРД используется понятие «оперативно-розыскная информация», под которой понимается непроцессуальная информация, получаемая в ходе производства ОРМ. Для лица, проводящего расследование, она носит вспомогательный, ориентирующий

характер¹. В основу названия «оперативно-розыскная информация» положен способ ее производства – ОРД, т. е. это информация, полученная определенным (оперативно-розыскным) образом².

Оперативно-розыскная информация – это сведения о лицах (сообществах физических лиц), предметах, документах, фактах, событиях, явлениях и процессах, получаемых в порядке, предусмотренном оперативно-розыскным законом и ведомственными нормативными актами по ОРД, зафиксированных на материальных носителях с реквизитами, позволяющими их идентифицировать, сосредоточиваемых в информационных системах и ДООУ.

Различные совокупности данной информации образуют имеющий конфиденциальный характер ресурс информационного обеспечения деятельности органов, осуществляющих ОРД.

Деятельность органов, осуществляющих ОРД, немыслима без использования специальных информационных технологий³.

Для информационного обеспечения ОРД создаются и используются различные виды учетов – оптимальные формы систематизации, в том числе оперативно-розыскной информации. Например: учет крупных и устойчивых организованных преступных формирований – единый автоматизированный банк данных в системе МВД России, включающий информацию об участниках и лидерах организованных преступных группировок, сферах их криминальной деятельности и другие оперативно-розыскные сведения; учет всех нераскрытых убийств, совершенных на территории РФ, в том числе имеющих серийный характер (информационно-аналитическая система «Глухарь»). Используются группы учетов, входящих в систему криминалистической (уголовной) регистрации, т. е. оперативно-справочные, криминалистические и розыскные учеты⁴. Оперативно-справочные учеты предназначены для проверки наличия установочных данных об объекте запроса; розыскные учеты выполняют, наряду с оперативно-справочными, функцию сравнения не только установочных данных,

¹ Гаврилин Ю.В., Головин А.Ю., Тишутина И.В. Криминалистика в понятиях и терминах: учеб, пособие / под ред. А.Ю. Головина. М., 2006. С. 24.

² Томин В.Т., Поляков М.П., Попов А.П. Очерки теории эффективности уголовного процесса. Пятигорск, 2000. С. 130.

³ Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (п. 2 ст. 2 ФЗ «Об информации»).

⁴ Понятие, содержание и правовые основы криминалистической (уголовной) регистрации подробнее см.: например: Драпкин Л.Я., Карагодин В.Н. Криминалистика: учеб. М., 2007. С. 148–170.

но и сходных внешних описаний; криминалистические учеты используются для диагностики и идентификации объектов по индивидуальным приметам и другим признакам, когда установочные данные неизвестны или скрываются.

В ст. 17 ФЗ «О полиции» представлен перечень сведений о гражданах, вносимых в банки данных, которые формируются и ведутся полицией.

Вид информации обусловлен видом объекта, о котором имеются сведения или о котором необходимо получить их (т. е. о лицах, фактических данных, событиях, предметах). Информация о лицах включает в себя сведения о лицах, подготавливающих, совершающих или совершивших преступление, скрывающихся от органов дознания, следствия, суда или уклоняющихся от уголовного наказания; без вести пропавших. Учету также подлежит информация об обнаружении неопознанных трупов, приметах неустановленных лиц, подозреваемых в совершении преступления. Информация о фактах включает в себя сведения о зарегистрированных преступлениях (раскрытых и нераскрытых). Подлежат учету события и действия, создающие угрозу государственной, военной, экономической, информационной, экологической безопасности России. Информация о предметах содержит сведения об орудиях и способах совершения преступления; огнестрельном оружии, которое находится в пользовании граждан и организаций; автотранспортных средствах; о разыскиваемых предметах, документах и вещах, явившихся предметом преступления.

Информационные системы представлены в различных формах: картотеки, фото-, видеотеки, коллекции, автоматизированные информационно-справочные, информационно-поисковые системы (автоматизированные банки данных).

Правовую основу функционирования информационно-поисковых систем составляют:

- ФЗ «Об ОРД» (ч. 1 ст. 10);
- ФЗ от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»;
- Наставление по формированию и ведению централизованных оперативно-справочных, криминалистических, розыскных учетов, экспертно-криминалистических коллекций и картотек органов внутренних дел РФ (утверждено приказом МВД России от 12 июля 2000 г. № 752);

– Инструкция по формированию и использованию экспертно-криминалистических учетов, картотек, коллекций и справочно-информационных фондов ОВД (утверждена приказом МВД России от 1 июня 1993 г. № 261);

– ФЗ «О полиции» (ст. 17);

– ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– межведомственный приказ Генпрокуратуры России, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений»;

– приказ МВД России от 8 декабря 2009 г. № 925 «Вопросы Главного информационно-аналитического центра МВД России».

С 2006 г. в соответствии с Инструкцией по организации формирования, ведения и использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации, утвержденной приказом МВД России от 10 февраля 2006 г. № 70, проводится работа по созданию на базе МВД России федеральных, а на базе Экспертно-криминалистического центра ОВД в субъектах РФ – региональных баз данных ДНК биологических объектов по преступлениям, предусмотренным ст. 105, 111, 131–135 УК РФ, а также по неопознанным трупам. Согласно ч. 1 ст. 15 Федерального закона от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» органы, осуществляющие ОРД, наделены правом использования *геномной информации*, под которой понимаются персональные данные, включающие кодированную информацию об определенных фрагментах ДНК физического лица или неопознанного трупа.

В 2012 г. в соответствии с приказом МВД России от 30 марта 2012 г. № 205 «Об утверждении Концепции создания единой системы информационно-аналитического обеспечения деятельности МВД России в 2012–2014 годах» началось формирование автоматизированных систем обработки информации, программно-технических средств, программно-аппаратных комплексов, а также систем связи и передачи данных, необходимых для обеспечения повседневной и служебной деятельности. ИСОД МВД России – единая система информационно-аналитического обеспечения деятельности МВД России включает в себя сервисы повседневной деятельности, межведомственного взаимодействия и оказания государственных услуг и оперативно-служебной деятельности.

Сервисы оперативно-служебной деятельности	
Следопыт-М	Информационно-поисковый сервис
СООП	Сервис обеспечения охраны общественного порядка
СОДЧ	Сервис обеспечения деятельности дежурных частей
СОМТО	Сервис обеспечения деятельности подразделений материально-технического обеспечения МВД России
ФИС ГИБДД-М	Федеральная информационная система ГИБДД МВД России
СОЭБ	Сервис обеспечения экономической безопасности
СОДИ	Сервис национального центрального бюро Интерпола
ЕАИС ЭКП	Сервис экспертно-криминалистической деятельности
СУОГЗ	Сервис обеспечения государственной защиты лиц
СОПС	Сервис оформления проезда сотрудников
СОПД ГУСБ	Сервис ГУ Собственной безопасности МВД России
МОСТ	Сервис статистической отчетности МВД России
ЦИАДИС-МВД	Банк отпечатков пальцев

Примерный план занятия

1. Сущность, задачи и правовые основания информационного обеспечения раскрытия и расследования преступлений.
2. Понятие информационного обеспечения ОРД, его виды и формы.
3. Роль и значение информационных систем органов внутренних дел в решении задач борьбы с преступностью.
4. Современные информационные поисковые системы и порядок их использования в раскрытии преступлений.
5. Классификация, виды и формы учетов.
6. Возможности использования учетов в противодействии преступлениям, совершаемым с использованием ИКТ.
7. Требования, предъявляемые к формированию учетов.
8. Запросы на получение сведений из информационных баз данных.

Вопросы для самоконтроля по теме

1. Каковы цели информационного обеспечения ОРД?
2. Для чего предназначены оперативно-справочные учеты?
3. Раскройте понятие оперативно-розыскной информации.
4. Назовите сервисы оперативно-служебной деятельности ИСОД МВД России.

Тема 2.11. Особенности документирования оперативно-розыскной деятельности органов внутренних дел при раскрытии преступлений

Правовая основа документирования ОРД

Согласно ст. 10 ФЗ «Об ОРД» правомерность и обоснованность деятельности органов, осуществляющих ОРД, предусматривает такой важнейший элемент их деятельности, как обязанность сотрудников оперативных подразделений документировать (фиксировать) результаты ОРД путем формирования информационных массивов сведений и отражения результатов ОРД в различного рода материалах и ДОУ.

Большинство положений данной статьи носят бланкетный (отсылочный) характер. Для их правильного уяснения и применения требуется руководствоваться предписаниями ведомственных НПА органов, осуществляющих ОРД.

Понятие, сущность, значение и содержание документирования

Эффективное противодействие организованной преступности не должно ограничиваться только тайным проникновением в среду правонарушителей и выявлением их целей и намерений. Гораздо более значимым является документирование (фиксация) на материальных носителях максимально полной, достоверной и объективной информации о готовящихся, совершаемых или совершенных противоправных деяниях, степени виновности причастных к ним лиц, на основе которой в установленном законом порядке можно принять к последним меры правового воздействия.

Документирование ОРД составляет одну из важных составных частей оперативно-розыскного производства.

Термин «документирование» может пониматься:

- 1) как неотъемлемая часть любой деятельности, направленная на собирание информации, которая потребуется в дальнейшем;
- 2) как технический процесс записи какой-либо информации на материальных носителях по определенным технологиям, формам и правилам;
- 3) как создание документа с использованием различных методов, способов и средств фиксации информации на материальном носителе.

Под документированием ОРД следует понимать выявление оперативно-розыскным путем фактических данных (сведений), свидетельствующих о причастности заподозренных и проверяемых лиц к приготовлению или совершению преступления, обеспе-

чение возможности использования этих данных для предупреждения или раскрытия преступления и принятия к виновным мер, предусмотренных законом.

Документирование ОРД позволяет:

– контролировать законность и обоснованность осуществления ОРД;

– использовать полученные материалы в процессе доказывания по уголовным делам.

В процессе документирования добываются не всякие фактические данные, а лишь такие, которые уличают преступника. Документирование может осуществляться либо в отношении конкретного лица, либо в отношении события. Круг фактических данных, которые в ходе документирования должны быть выявлены и задокументированы, определяется обстоятельствами, подлежащими доказыванию по уголовному делу (ст. 73 УПК РФ), в первую очередь теми из них, которые характеризуют объективную сторону преступления. Данные обстоятельства неодинаковы по своей природе. Поэтому содержание документирования может быть различным в зависимости от вида преступления и конкретных задач ОРД.

Документирование ОРД осуществляется в отдельных организационно-тактических формах:

- 1) предварительной оперативной проверки;
- 2) оперативной разработки;
- 3) оперативно-розыскного обеспечения предварительного расследования преступлений и их судебного рассмотрения;
- 4) оперативно-розыскного противодействия лицам, занимающим высшее положение в преступной иерархии, лидерам экстремистских сообществ (организаций), террористических организаций и незаконных вооруженных формирований;
- 5) оперативно-розыскного обеспечения государственной защиты;
- 6) розыска лиц, скрывшихся от следствия, органа дознания и суда;
- 7) оперативно-розыскного обеспечения розыска без вести пропавших лиц;
- 8) оперативно-розыскного обеспечения идентификации личности;
- 9) оперативно-розыскного обеспечения исполнения запросов международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами Российской Федерации;
- 10) оперативно-розыскного обеспечения собственной безопасности в системе МВД России.

Предварительная оперативная проверка представляет собой комплекс ОРМ, направленных на установление достоверности первичной оперативной и иной информации о признаках подготавливаемого, совершаемого или совершенного преступления, о лицах, их подготавливающих, совершающих или совершивших, а также на сбор дополнительных сведений о них для решения задач ОРД.

Предварительная оперативная проверка первичной информации позволяет установить определенные факты (явления, события, действия), указывающие на подготовку или совершение противоправных деяний конкретными лицами. По результатам предварительной оперативной проверки должностными лицами оперативных подразделений могут быть приняты следующие решения:

- о проведении ОРМ по предупреждению (пресечению) подготавливаемого (совершаемого) преступления;
- о проведении оперативной разработки;
- о возбуждении уголовного дела;
- о направлении собранных материалов по подследственности или территориальности;
- о прекращении проверки в связи с неподтверждением первичных сведений, послуживших поводом для ее проведения.

Оперативная разработка осуществляется в отношении достигших возраста уголовной ответственности лиц в целях сбора дополнительных сведений, которые в дальнейшем могут быть использованы в качестве доказательств по уголовному делу, при наличии проверенной информации о причастности данных лиц к подготовке или совершению преступлений. Оперативная разработка предполагает осуществление комплекса ОРМ преимущественно негласного характера, проводимых при наличии обоснованных данных о признаках подготавливаемых, совершаемых или совершенных преступлений, по которым производство предварительного следствия обязательно, в целях их пресечения или раскрытия, когда иными мерами гласного характера достичь указанных целей невозможно или крайне затруднительно.

Необходимость производства оперативной разработки возникает в том случае, когда нет формальных оснований для принятия процессуального решения о возбуждении уголовного дела, однако имеются достоверные (проверенные, подтвержденные) сведения о причастности того или иного лица (группы лиц) к преступной деятельности.

Оперативно-розыскное обеспечение предварительного расследования и рассмотрения уголовных дел в суде представляет со-

бой комплекс ОРМ, проводимых на основании возбужденного уголовного дела и направленных на установление лиц, совершивших в условиях неочевидности преступление, а также на своевременное и полное информирование предварительного следствия об обстоятельствах расследуемых преступлений, фактах противодействия расследованию и рассмотрению уголовных дел в суде. Вся работа по нераскрытым преступлениям строится на основе выдвижения криминалистических версий и их проверки путем проведения согласованных следственных действий и ОРМ в рамках возбужденного уголовного дела и соответствующего ДОУ, заведенного для осуществления оперативного сопровождения его предварительного расследования.

Оперативно-розыскное противодействие лицам, занимающим высшее положение в преступной иерархии (в том числе лидерам экстремистских сообществ, террористических организаций и незаконных вооруженных формирований), представляет собой сбор, анализ и оценку материалов специального наблюдения за указанной категорией криминальных элементов в целях своевременного выявления и нейтрализации их преступных намерений. Так как лидеры преступной среды (криминальные авторитеты) вследствие их статуса постоянно вовлечены в противоправную деятельность, необходимо постоянно контролировать их действия (наблюдать за перемещением, отслеживать контакты и связи, в том числе коррумпированные, устанавливать каналы финансирования возглавляемых ими преступных сообществ и т. д.).

Оперативно-розыскное обеспечение государственной защиты заключается в проведении комплекса ОРМ в связи с применением мер безопасности в отношении защищаемых лиц в соответствии с Федеральными законами от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства». В целях выявления и пресечения преступлений, совершаемых в отношении защищаемых лиц, проводятся ОРМ по документированию фактов угроз и посягательств на жизнь, здоровье, имущество, близких и родных этих лиц. На основании полученных материалов принимается решение о предупреждении подготавливаемого или пресечении совершаемого преступления и привлечении виновных к уголовной ответственности.

Розыск лиц, скрывшихся от следствия, органа дознания и суда предполагает проведение ОРМ по установлению местонахожде-

ния скрывшихся преступников и в зависимости от оперативно-тактической ситуации – их задержание и доставление. В ходе проведения ОРМ осуществляется документирование сведений:

- о разыскиваемых преступниках, местах их возможного появления, нахождения (укрытия);
- о лицах, которые обладают информацией, представляющей оперативный интерес;
- о фактах (событиях, явлениях), имеющих отношение к разыскиваемому лицу и способствующих эффективному осуществлению розыска.

Оперативно-розыскное обеспечение розыска без вести пропавших лиц предполагает проведение ОРМ по установлению местонахождения различных категорий лиц, исчезнувших внезапно, без видимых на то причин, местонахождение которых не известно. Розыск осуществляется в целях спасения этих лиц, оказания помощи и т. д. В ходе проведения ОРМ осуществляется документирование сведений:

- о пропавших без вести лицах (их приметы, во что были одеты и т. д.);
- о лицах, которые обладают информацией, позволяющей установить местонахождение разыскиваемого;
- о предметах (документах, вещах), свидетельствующих об обстоятельствах криминального исчезновения разыскиваемого лица.

Оперативно-розыскное обеспечение идентификации личности по своей сути имеет определенное методическое сходство с предыдущими двумя организационно-тактическими формами, обеспечивающими розыск скрывшихся преступников и без вести пропавших лиц. Однако если розыскная работа осуществляется по тактической схеме – от события исчезновения (сокрытия) лица до обнаружения его местонахождения, то идентификационная работа проводится по обратной схеме – от обнаружения неопознанного лица или трупа до установления его личности и событий, предшествующих его обнаружению.

Оперативно-розыскное обеспечение исполнения запросов международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами Российской Федерации осуществляется в целях:

- эффективного международного обмена информацией об уголовных преступлениях;

– оказания содействия в исполнении запросов международных правоохранительных организаций и правоохранительных органов иностранных государств на основании ранее достигнутых соглашений и заключенных международных договоров;

– выявления и установления на территории Российской Федерации лиц, причастных к преступной деятельности международного характера.

Оперативно-розыскное обеспечение собственной безопасности в системе МВД России осуществляется в целях выявления, предупреждения и раскрытия следующих преступлений:

– подготавливаемых, совершаемых или совершенных сотрудниками ОВД, федеральными государственными гражданскими служащими и работниками системы МВД России;

– создающих угрозы собственной безопасности системы МВД России.

Наиболее распространенным результатом документирования традиционно является оперативно-служебный документ (рапорт, справка, акт, объяснение, постановление, план, сводка и т. д.), но им может быть и любой другой носитель информации (фотография, оптический диск, флеш-карта и т. д.). В современных условиях все большее значение приобретают электронные документы, а также документы, полученные в результате работы технических устройств: файлы-записи камер наблюдения, фотографии и переписка в мессенджерах и социальных сетях; документы, отражающие сведения о движении средств по счетам, о телефонных соединениях, посещенных интернет-ресурсах, месте нахождения абонентского устройства сотовой связи, сведения об использовании устройств выхода в Интернет и т. д.

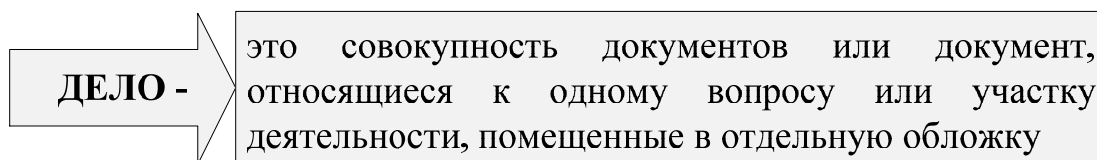
Оперативно-служебный документ – материальный носитель с зафиксированными фактическими данными (информацией, сведениями), полученными в процессе ОРД и оформленными по установленным в оперативно-розыскных органах правилам делопроизводства, включая наличие определенных реквизитов.

Электронный документ – документированная информация, представленная в электронной форме, т. е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по ИТКС или обработки в информационных системах (п. 11.1 ст. 2 ФЗ «Об информации»).

Согласно ГОСТ Р 7.0.83 **электронный документ** – это документ в цифровой форме, для использования которого необходимы СВТ или иные специализированные устройства для воспроизведения текста, звука, изображения.

Виды дел оперативного учета, основания и порядок их ведения

В рамках каждой из перечисленных выше организационно-тактических форм заводятся соответствующие им дела.

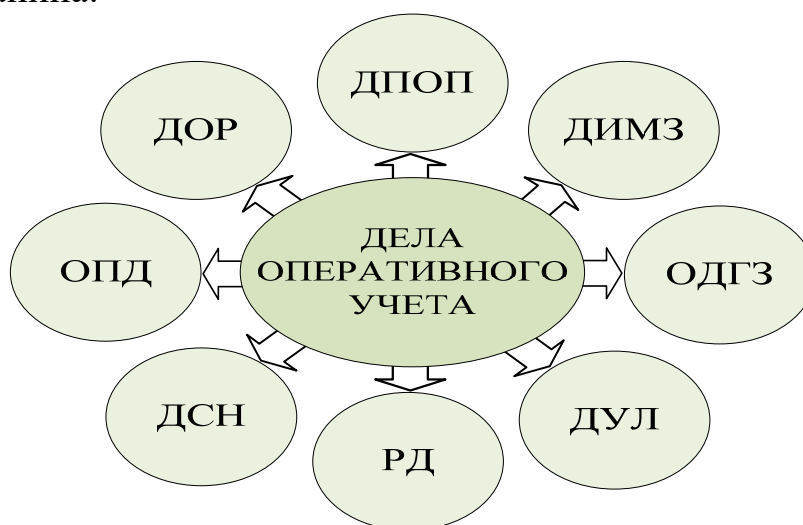


Результаты документирования ОРД помещаются в соответствующие ДООУ или дела накопительно-наблюдательного производства. Эти дела следует отличать от уголовных и других дел, так как они формируются по правилам секретного делопроизводства и не влекут наступления юридически значимых последствий для лиц, проходящих по ним.

Дела оперативного учета могут заводиться в целях собирания и систематизации сведений, проверки и оценки результатов ОРД, а также принятия на их основе соответствующих решений.

Основаниями заведения ДООУ являются те же основания, что предусмотрены для проведения ОРМ, а именно пп. 1–6 ч. 1 ст. 7 ФЗ «Об ОРД».

Факт заведения ДООУ не является основанием для ограничения конституционных прав и свобод, а также законных интересов человека и гражданина.



ДПОП	→	Дело предварительной оперативной проверки
ДОР	→	Дело оперативной разработки
ОПД	→	Оперативно-поисковое дело
ДСН	→	Дело специального наблюдения
РД	→	Розыскное дело
ДУЛ	→	Дело по установлению личности
ОДГЗ	→	Оперативное дело государственной защиты
ДИМЗ	→	Дело по исполнению международных запросов

Дела оперативного учета заводятся для установления определенных фактов (явлений, событий) противоправных действий либо по признакам конкретных составов преступлений, проверка обстоятельств вероятного совершения которых относится к оперативно-розыскной подведомственности соответствующего оперативно-розыскного органа.

Заведение ДОУ связано с вынесением постановления соответствующим должностным лицом с последующим обязательным утверждением руководителем оперативно-розыскного органа.

Решения, принимаемые по материалам ДОУ, оформляются в виде постановлений: о его заведении, продлении, прекращении или возобновлении. Постановление может быть вынесено и в других случаях, предусмотренных ведомственными нормативными актами (например, при соединении ДОУ в одно производство; при постановке лица, проходящего по ДОУ, на централизованный учет или снятии его с учета; при объявлении лица, проходящего по ДОУ, в розыск).

Решение о прекращении ДОУ принимается руководителем оперативно-розыскного органа в связи с наличием на то достаточных оснований. Часть 4 ст. 10 ФЗ «Об ОРД» предусматривает два вида оснований:

1) решение конкретных задач ОРД, предусмотренных ст. 2 ФЗ «Об ОРД»;

2) установление обстоятельств, свидетельствующих об объективной невозможности решения этих задач.

По второму основанию ДОУ подлежат прекращению:

- при неподтверждении сведений, на основании которых было заведено ДОУ;
- при декриминализации общественно опасного деяния, в связи с вероятным совершением которого на лицо было заведено ДОУ;
- по акту амнистии, если он устраняет применение наказания за преступление, совершенное лицом, в отношении которого было заведено ДОУ;
- при прекращении уголовного дела вследствие истечения срока давности уголовного преследования;
- при получении достоверных сведений о смерти лица, в отношении которого было заведено ДОУ;
- при поступлении проверенных сведений и объективных данных об отказе лица, в отношении которого было заведено ДОУ, от своего криминального статуса и положения.

Особенности документирования ОРД органов внутренних дел при раскрытии преступлений

Документирование ОРД при раскрытии преступлений по организационно-тактической схеме «от лица – к преступлению» или «от преступления – к лицу» имеет свои особенности. По схеме «от преступления – к лицу» документирование ОРД осуществляется при наличии возбужденного уголовного дела, направлено на обеспечение оперативного сопровождения расследования преступления и предполагает незамедлительное введение полученных оперативным путем сведений в уголовный процесс для их дальнейшего использования при отработке и корректировке версий, выборе времени, места и тактики проведения отдельных следственных действий.

Проводимые мероприятия направлены:

- на установление лиц, причастных к совершенному преступлению, путем их оперативного распознавания на основании имеющихся в распоряжении следствия поисковых признаков;
- поиск материальных объектов, имеющих значение для раскрытия преступления и могущих быть вещественными доказательствами причастности тех или иных лиц к совершенному преступлению;
- установление возможных свидетелей и очевидцев преступления, чьи показания будут иметь существенное значение в раскрытии преступления и рассмотрении уголовного дела в суде.

Все полученные оперативные материалы в установленном порядке представляются следователю для их приобщения к материалам уголовного дела и использования в процессе доказывания. Результаты

документирования ОРД, отражающие факты противодействия объективному судебному разбирательству (подкуп или запугивание свидетелей и потерпевших, уничтожение или порча вещественных доказательств и т. д.), представляются в суд для учета и принятия соответствующего решения.

При раскрытии преступлений по тактической схеме «от лица – к преступлению» документирование ОРД осуществляется задолго до решения вопроса о возбуждении уголовного дела. Временной разрыв между моментом получения оперативным путем необходимых для раскрытия преступления сведений и началом их реализации в уголовном процессе может быть достаточно большим, а в ходе работы по делам оперативного учета может исчисляться годами. В рамках данной тактической схемы документирование ОРД осуществляется в условиях глубокой конспирации, когда полученные оперативно-розыскные данные невозможно незамедлительно закрепить уголовно-процессуальным путем, а также когда незамедлительное введение полученных оперативным путем сведений в уголовный процесс не оправдано по тактическим соображениям.

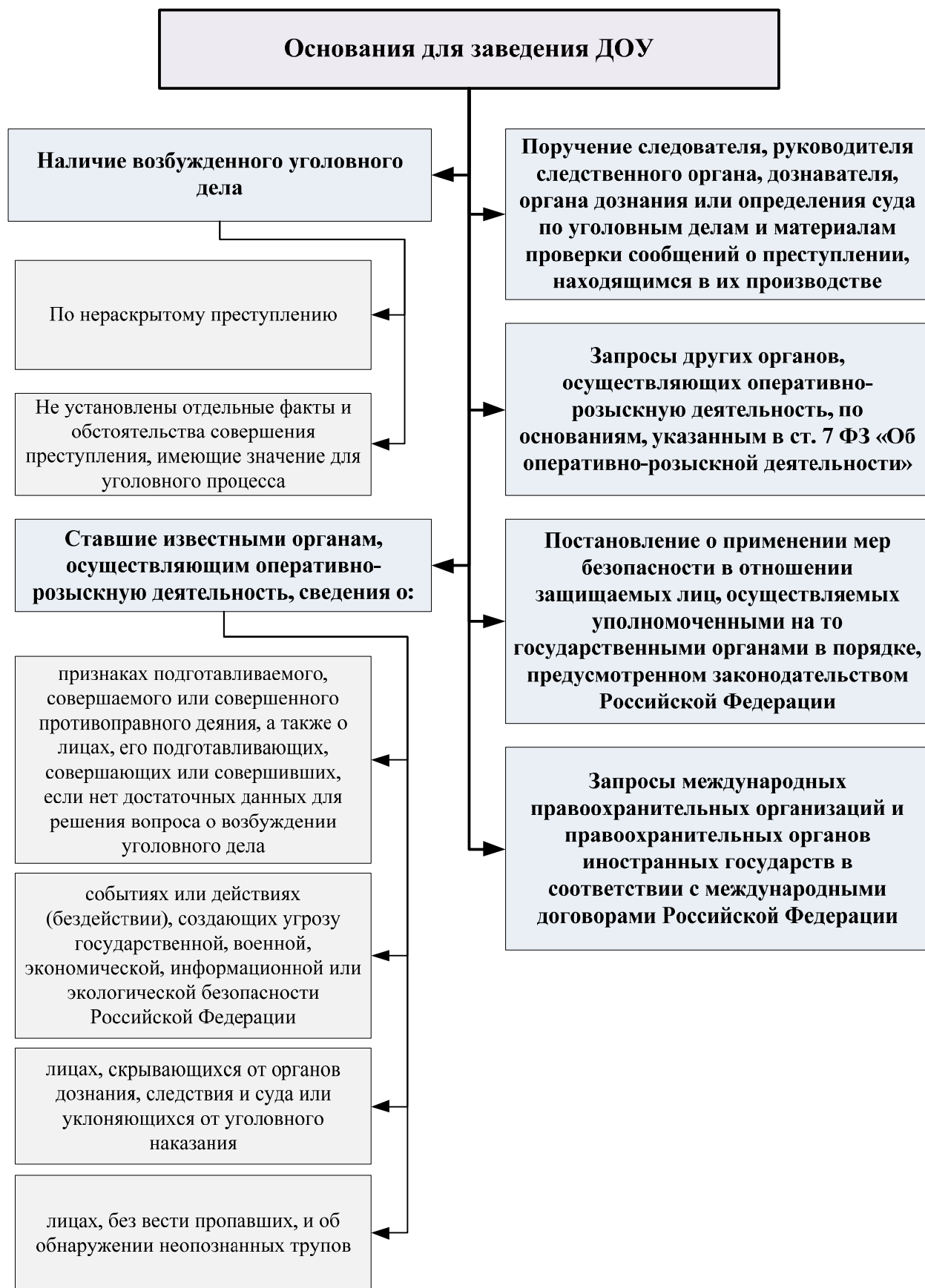
Поскольку документирование ОРД направлено на обеспечение процесса доказывания по уголовным делам, основные направления этой деятельности напрямую вытекают из положений уголовно-процессуального законодательства об источниках доказательственной информации (см. подробнее ст. 74 УПК РФ).

Обстоятельства, составляющие предмет документирования (он совпадает с предметом доказывания), выявляют и закрепляют путем осуществления ОРМ по трем основным направлениям:

1) выявление лиц, которые могут быть свидетелями по уголовному делу;

2) обнаружение предметов и документов, содержащих признаки преступной деятельности, которые могут быть использованы в качестве вещественных доказательств по уголовному делу;

3) фиксация преступных действий лиц в целях последующего использования полученных данных в процессе расследования преступления.



Примерный план занятия

1. Правовая основа документирования оперативно-розыскной деятельности.
2. Понятие, сущность, значение и содержание документирования.
3. Виды дел оперативного учета, основания и порядок их ведения.
4. Особенности документирования оперативно-розыскной деятельности органов внутренних дел при раскрытии преступлений.

Вопросы для самоконтроля по теме

1. Понятие и объекты учетов, используемых в оперативно-розыскной деятельности органов внутренних дел.
2. Виды и формы учетов, используемых в оперативно-розыскной деятельности органов внутренних дел.
3. Информационно-аналитическая работа в оперативно-розыскной деятельности органов внутренних дел.
4. Основные задачи ГИАЦ МВД России.
5. Общие положения производства по делам оперативного учета.

Тема 2.12. Использование результатов оперативно-розыскной деятельности

Понятие результатов ОРД

В соответствии с п. 36 ст. 5 УПК РФ результаты ОРД – это сведения, полученные в соответствии с ФЗ «Об ОРД», о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда.

Оперативно-розыскная деятельность и уголовное судопроизводство представляют собой единство процессуального и непроцессуального. Это единство заключается не только в проведении следственных действий или ОРМ, но и предполагает наряду с добыванием информации ее использование, принятие решений как процессуального, так и оперативно-розыскного характера. Например, результаты проверочной закупки могут служить основанием для принятия процессуальных решений (возбуждение уголовного дела) и (или) проведения следственных действий (обыск, выемка, осмотр места происшествия).

Основные направления использования результатов ОРД

Согласно ч. 1–3 ст. 11 ФЗ «Об ОРД» результаты ОРД могут быть использованы:

- для подготовки и осуществления следственных и судебных действий;
- в качестве повода и основания для возбуждения уголовного дела;
- в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства РФ, регламентирующими собирание, проверку и оценку доказательств;
- налоговыми органами при реализации ими полномочий по контролю и надзору за соблюдением законодательства о налогах и сборах, по обеспечению представления интересов государства в делах о банкротстве, а также при реализации полномочий в сфере государственной регистрации юридических лиц.

В ОРД при проведении даже одного ОРМ может достигаться решение конкретной оперативно-розыскной задачи, например, выявление признаков преступления. Результатом служит наличие конкретной и достоверной информации о преступлении, которой может быть достаточно для возбуждения уголовного дела, проведения следственных действий, хотя такая информация не обязательно должна

быть использована в уголовно-процессуальном порядке либо используется не сразу.

Принятие процессуальных решений, основанных на результатах ОРД, либо проведение следственных действий может осуществляться лишь после проведения ряда ОРМ, например наблюдения, оперативного внедрения, проверочной закупки, ПТП, контролируемой поставки, даже если результаты любого из них уже сами по себе могли служить основанием для процессуальных решений и действий.

Использование результатов ОРД для подготовки и осуществления процессуальных действий

Под использованием результатов ОРД для осуществления следственных действий следует понимать возможность учета указанных результатов как при принятии решения о производстве этих действий, так и при непосредственном их проведении.

Так, в соответствии со ст. 182 УПК РФ обыск производится при наличии достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться объекты, имеющие значение для уголовного дела: орудия преступления, предметы, документы и ценности, разыскиваемые лица и трупы. Оперативно-розыскные данные могут дополнять имеющуюся совокупность процессуальных сведений о нахождении в определенном месте или у какого-либо лица искомых следователем объектов, что поможет следователю в процессе принятия решения о производстве обыска, а также поможет в его подготовке и проведении.

В процессе подготовки к допросу (очной ставке) результаты деятельности оперативных работников призваны обеспечить выполнение задач, имеющих важное значение для получения полных и правдивых показаний: установление свидетелей, выяснение взаимоотношений между ними, а также взаимоотношений между свидетелями и подозреваемыми и др. В общем, результаты ОРД, используемые для подготовки к допросу (очной ставке), – это те, что содержат информацию, способствующую всестороннему изучению личности допрашиваемых (сведения об образе жизни, круге их связей, намерениях и т. д.).

Аналогично результаты ОРД могут использоваться для принятия решения о задержании, а также о производстве таких следственных действий, как осмотр, получение образцов для сравнительного исследования, эксгумация, освидетельствование, выемка, наложение ареста на почтово-телеграфные отправления, назначение и производство экспертизы, получение информации о соединениях между абонентами и (или) абонентскими устройствами.

Результаты ОРД, представляемые для подготовки и осуществления следственных действий, должны содержать информацию о лицах, скрывающихся от органов дознания, следствия и суда; сведения, которые можно получить из определенных процессуальных источников; данные о местонахождении орудий и средств преступления, денег и иного имущества, полученных преступным путем, предметах и документах, связанных с обстоятельствами, подлежащими доказыванию; другие данные, позволяющие определить круг и последовательность проведения процессуальных действий, избрать эффективную тактику их производства, составить методику расследования по данному уголовному делу.

В подготовке и осуществлении судебных действий результаты ОРД могут быть учтены судом, например, при решении вопроса об изменении меры пресечения подсудимому, когда в них имеются фактические данные о препятствии подсудимого судебному разбирательству.

Нормативно-правовые основания предоставления результатов ОРД в орган дознания, следователю или в суд

Порядок предоставления результатов ОРД в орган дознания, следователю или в суд регламентирован межведомственным приказом МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, Следственного комитета РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

Согласно п. 19 данной Инструкции результаты ОРД, представляемые для подготовки и осуществления следственных и судебных действий, должны содержать сведения о местонахождении лиц, скрывающихся от органов предварительного расследования и суда; о лицах, которым известны обстоятельства и факты, имеющие значение для уголовного дела; о возможных источниках доказательств; о местонахождении предметов, перечисленных в ч. 1 ст. 81 УПК РФ; о других фактах и обстоятельствах, позволяющих определить объем и последовательность проведения процессуальных действий, выбрать наиболее эффективную тактику их производства, выработать оптимальную методику расследования по конкретному уголовному делу.

Использование результатов ОРД в качестве повода и основания для возбуждения уголовного дела

Уголовно-процессуальный закон прямо не предусматривает результаты ОРД в качестве повода и основания для возбуждения уголовного дела, но косвенно говорит о них. Так, в п. 3 ч. 1 ст. 140 УПК РФ предусматривается в качестве повода для возбуждения уголовного

дела сообщение о совершенном или готовящемся преступлении, полученное из любых источников, не связанных с заявлением о преступлении или явкой с повинной. Таким источником может быть, в частности, рапорт об обнаружении признаков преступления (ст. 143 УПК РФ), составленный конкретным должностным лицом, получившим соответствующую информацию (фактические данные), указывающую на подготовку или совершение деяния, подпадающего под признаки какого-либо преступления.

Согласно постановлению Конституционного суда РФ от 6 ноября 2014 г. № 27-П результаты ОРД являются вспомогательным средством для установления юридически значимых фактов и обстоятельств, имеющих значение для принятия предусмотренного ст. 145 УПК РФ процессуального решения по результатам рассмотрения сообщения о преступлении.

Результаты ОРД могут служить поводом для возбуждения уголовного дела в случае получения субъектом ОРД информации в процессе проведения ОРМ при проверке заявления о преступлении или оперативной информации из конфиденциальных источников, мероприятий, обеспечивающих проведение следственных действий в ходе расследования других преступлений.

Согласно п. 18 Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд результаты ОРД, представляемые для решения вопроса о возбуждении уголовного дела, должны содержать достаточные данные, указывающие на признаки преступления, а именно: сведения о том, где, когда, какие признаки и какого именно преступления обнаружены; при каких обстоятельствах имело место их обнаружение; сведения о лице (лицах), его совершившем (если оно известно), и очевидцах преступления (если они известны); о местонахождении предметов и документов, которые могут стать вещественными доказательствами; о любых других фактах и обстоятельствах, имеющих значение для решения вопроса о возбуждении уголовного дела. Сведения, содержащиеся в представляемых результатах, должны позволять сделать вывод о наличии события и его противоправности или, иными словами, должны содержать достаточные данные, указывающие на признаки преступления.

Использование результатов ОРД в доказывании по уголовным делам

Результаты ОРД не являются доказательствами, так как они не соответствуют требованиям УПК РФ. Доказательство должно отве-

чать трем требованиям, которые предъявляются соответственно к его содержанию и форме – относимости, допустимости и достоверности. Результаты ОРД могут отвечать требованию относимости, т. е. содержать сведения о фактах и обстоятельствах, имеющих значение для уголовного дела. Поскольку эти данные получаются из источников и способами, не предусмотренными уголовно-процессуальным законом, их нельзя считать отвечающими требованию допустимости. Поэтому результаты ОРД могут служить основой для формирования (собираания) доказательств в уголовном процессе, а также создавать условия и предпосылки для их установления. Результаты ОРД станут доказательствами только тогда, когда окажутся в соответствующих процессуальных источниках, обозначенных в ч. 2 ст. 74 УПК РФ, посредством проведения соответствующих следственных действий.

В определении Конституционного суда РФ от 4 февраля 1999 г. № 17-0 разъяснено, что непосредственные результаты ОРМ являются не доказательствами, а лишь сведениями об источниках тех фактов, которые, будучи полученными с соблюдением требований ФЗ «Об ОРД», могут стать доказательствами только после закрепления их надлежащим процессуальным путем, а именно на основе соответствующих норм уголовно-процессуального закона. В Определении от 1 декабря 1999 г. № 211-0 Конституционный суд РФ отметил, что проведение ОРМ, сопровождающих производство предварительного расследования по уголовному делу, не может подменять процессуальные действия, предусмотренные уголовно-процессуальным законом.

Требования, предъявляемые к результатам ОРД, предоставляемым органу дознания, следователю или в суд

Результаты ОРД являются доказательствами, если они получены и проверены в порядке, предусмотренном Законом «Об ОРД», и содержат сведения, имеющие значение для установления обстоятельств, указанных в ст. 73 УПК РФ. Результаты ОРД представляются органу дознания, следователю или в суд органом, осуществляющим ОРД, в виде подлинных оперативно-служебных материалов, копий и других предметов и документов. Они должны быть осмотрены и приобщены к уголовному делу постановлением органа дознания, следователя, судьи или определением суда. К результатам ОРД, обладающим признаками, указанными в ст. 81 УПК РФ, применяются правила, предусмотренные ст. 82 УПК РФ. В случаях, связанных с необходимостью обеспечения безопасности лиц, предоставивших информацию органу, осуществляющему ОРД, допускается допрос должностного лица, которому достоверно известно происхождение проверяемых данных и которое должно засвидетельствовать их подлинность и обстоятельства получения. Результаты ОРД, не соответствующие требованиям,

изложенным в ч. 1 ст. 82 УПК РФ, возвращаются в орган, осуществляющий ОРД. В случае необходимости орган дознания, руководитель следственного органа, следователь и суд направляют Оперативно-розыскному органу поручение, в котором называются недостатки, подлежащие устранению.

Если в ходе ОРД были допущены нарушения закона, то доказательства, основанные на результатах ОРД, полученных с нарушением положений ФЗ «Об ОРД», не будут признаны судом допустимыми.

Согласно п. 20 Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд результаты ОРД, представляемые для использования в доказывании по уголовным делам, должны позволять формировать доказательства, удовлетворяющие требованиям уголовно-процессуального законодательства в целом к соответствующим видам доказательств; содержать сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию по уголовному делу; содержать указания на ОРМ, при проведении которых получены предполагаемые доказательства, а также данные, позволяющие проверить в условиях уголовного судопроизводства доказательства, сформированные на их основе.

Примерный план занятия

1. Понятие результатов ОРД.
2. Основные направления использования результатов ОРД, закрепленные в Законе «Об ОРД».
3. Нормативно-правовые основания представления результатов ОРД в органы дознания, следователю или в суд.
4. Требования, предъявляемые к результатам ОРД, представляемым органу дознания, следователю или в суд.
5. Документальное оформление представления результатов ОРД.

Вопросы для самоконтроля по теме

1. Понятие и сущность использования результатов ОРД.
2. Особенности использования результатов ОРД.
3. Правовые основы использования результатов ОРД в уголовном судопроизводстве.
4. Порядок представления результатов ОРД органу дознания, следователю или в суд.
5. Формы представления результатов ОРД.
6. Алгоритм проверки и оценки результатов ОРД.

Тема 2.13. Взаимодействие оперативных подразделений органов внутренних дел с другими субъектами оперативно-розыскной деятельности и иными государственными органами

Нормативная основа взаимодействия оперативных подразделений ОВД с другими субъектами ОРД и иными государственными органами представляет собой совокупность законодательных и подзаконных нормативных актов. К их числу следует отнести: Конституцию РФ, международные договоры Российской Федерации по вопросам взаимодействия правоохранительных органов в сфере борьбы с преступностью, уголовное и уголовно-процессуальное законодательство, оперативно-розыскное законодательство, межведомственные и ведомственные нормативные правовые акты, регулирующие вопросы взаимодействия.

Ведомственные нормативные правовые акты МВД России, определяющие организацию и тактику взаимодействия между различными службами и подразделениями ОВД, можно подразделить на следующие виды:

- носящие общий директивный характер (решения коллегии, директивы МВД, определяющие задачи всех служб и подразделений);
- направленные на организацию работы по решению конкретных проблем (например, по борьбе с проявлениями организованной преступности в сфере компьютерной информации);
- посвященные совершенствованию организации работы по борьбе с преступностью на конкретных территориях (регионах);
- регламентирующие организацию и тактику борьбы с отдельными видами преступлений;
- освещающие взаимодействие отдельных подразделений.

Примером ведомственных НПА может служить Инструкция по организации совместной оперативно-служебной деятельности подразделений органов внутренних дел Российской Федерации при раскрытии преступлений и расследовании уголовных дел¹.

Межведомственные нормативные правовые акты, регламентирующие вопросы взаимодействия, условно можно подразделить на:

- на нормативные акты, регламентирующие взаимодействие оперативных служб различных ведомств;

¹ Утверждена приказом МВД России от 29.04.2015 № 495/дсп.

– нормативные акты, регламентирующие взаимодействие оперативных подразделений ОВД и других правоохранительных органов (например, совместные приказы МВД России и Генеральной прокуратуры РФ);

– нормативные акты, регламентирующие взаимодействие органов внутренних дел и государственных органов.

К числу межведомственных НПА можно отнести Инструкцию о порядке представления результатов ОРД органу дознания, следовательно или в суд¹.

Понятие, виды и формы взаимодействия

Взаимодействие между службами и подразделениями ОВД, а также иными субъектами является одним из важных элементов организации их деятельности. Как правило, необходимость взаимодействия возникает только тогда, когда одна из сторон взаимодействия:

а) обладает познаниями, которыми другая сторона не обладает;

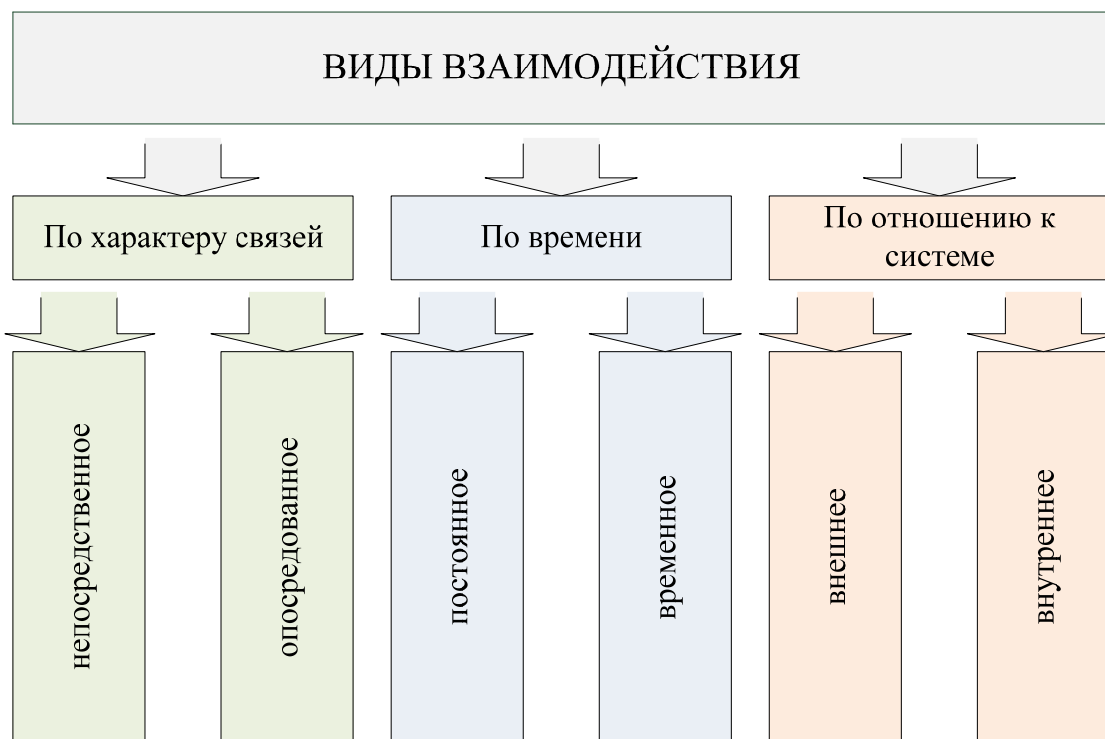
б) имеет возможности, которых у другой стороны нет.

Взаимодействие – это основанная на законах и подзаконных нормативных актах согласованная по целям, месту и времени деятельность неподчиненных друг другу различных служб и подразделений, направленная на решение локальных задач борьбы с преступностью путем наиболее целесообразного использования сил, средств и методов, имеющихся в их распоряжении.

Взаимодействие обусловлено:

- единством объекта взаимодействия (преступность);
- единством цели и общностью задач в раскрытии и расследовании преступлений;
- практической потребностью во взаимодействии;
- взаимной заинтересованностью в достижении целей;
- согласованностью или совместностью действий;
- самостоятельностью субъектов в выборе сил и средств;
- возможностью достижения максимально эффективных результатов в борьбе с преступностью при комплексном использовании сил и средств;
- оказанием взаимной помощи и содействия;
- взаимным информированием о ходе и результатах взаимодействия;
- совместной ответственностью за установленные правила и результаты взаимодействия.

¹ Утверждена приказом МВД России, МО России, ФСБ России, ФСО России, ФТС, СВР России, ФСИН России, ФСКН России, СК России от 27.09.2013 № 776/703/509/507/1820/42/535/398/68.



По характеру связей взаимодействие может быть:

- непосредственным – установление прямых связей между взаимодействующими субъектами (например, деятельность следственно-оперативной группы);

- опосредованным – связь между субъектами и подразделениями осуществляется через вышестоящий орган, представляющий ту службу, в интересах которой организуется взаимодействие.

По времени взаимодействие может быть:

- постоянным – осуществляется в течение всей работы по предупреждению и раскрытию преступлений;

- временным – направлено на решение небольших по объему конкретных задач, которые выполняют, например, следственно-оперативные группы при раскрытии отдельных преступлений.

По отношению к системе взаимодействие может быть:

- внешним – согласованная деятельность с иными службами не системы МВД (оперативные части СИЗО, ИК; оперативные подразделения ФСБ, прокуратура, Следственный комитет);

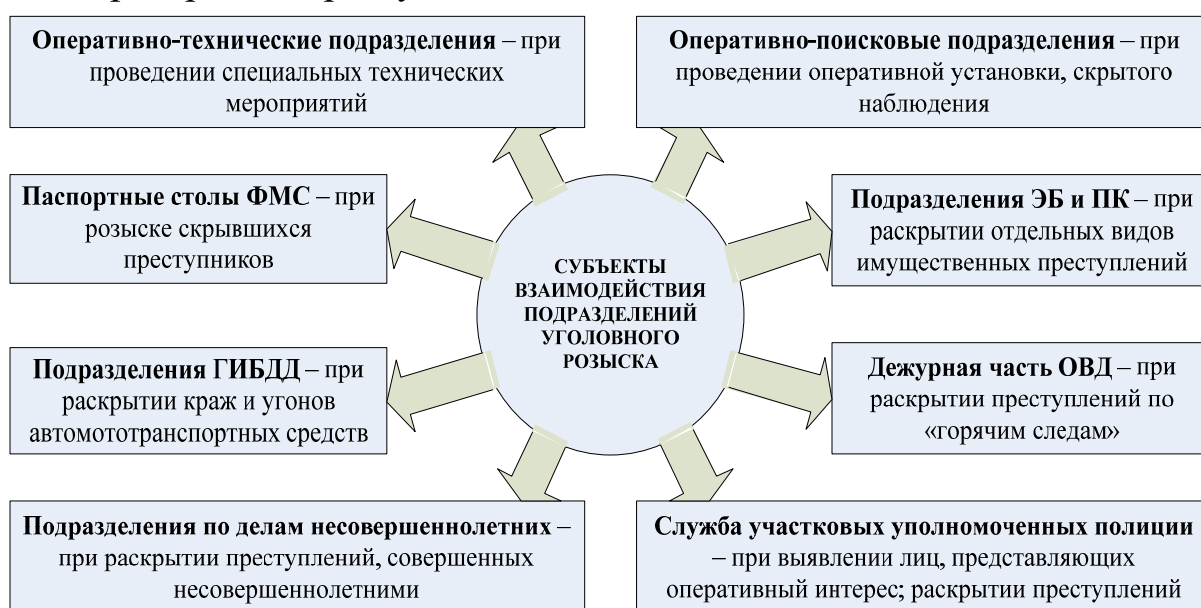
- внутренним – согласованная деятельность со службами, являющимися структурными подразделениями ОВД (участковые уполномоченные полиции, ГИБДД, дежурные части и т. д.).



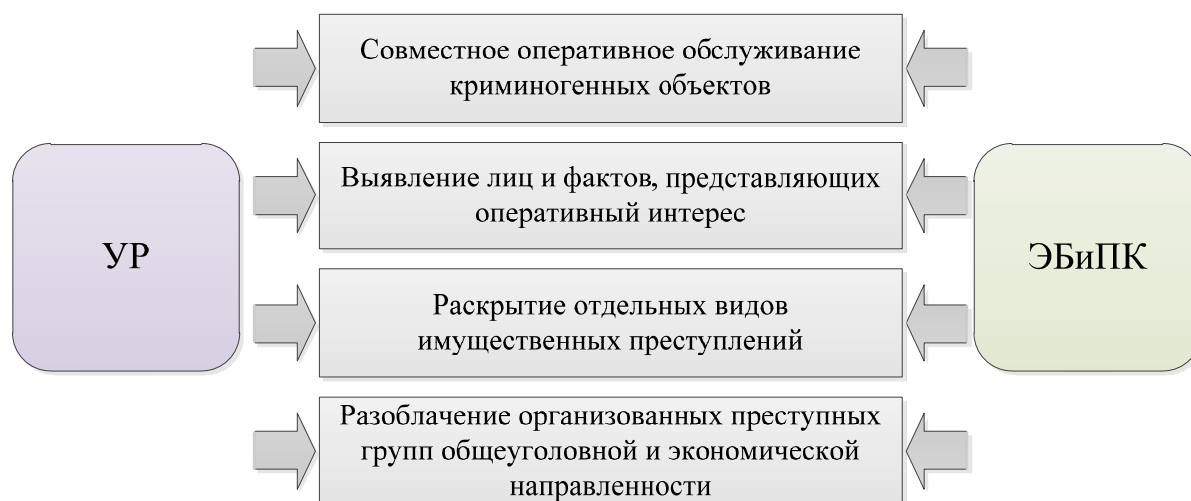
В качестве субъектов взаимодействия должны выступать все службы и подразделения органов внутренних дел, другие государственные органы, общественные формирования.

Взаимодействие оперативных подразделений с иными службами и подразделениями органов внутренних дел

Взаимодействие – это сложный процесс, охватывающий различные направления оперативно-служебной деятельности, важнейшими условиями которой являются расширение и углубление сотрудничества между оперативными подразделениями и правильная организация их совместной работы при выявлении, предупреждении, пресечении и раскрытии преступлений.



Выбор форм и субъектов взаимодействия зависит от конкретных задач, решаемых оперативным подразделением в текущий момент. Например, при необходимости негласного сбора информации, в том числе с помощью специальных технических средств, в целях раскрытия преступления оперативные подразделения уголовного розыска, ЭбиПК, ЦПЭ, УСБ используют возможности оперативно-поисковых и оперативно-технических подразделений, которые проводят в пределах своих полномочий оперативно-поисковые, оперативно-технические, оперативно-аналитические мероприятия. При раскрытии преступлений по горячим следам оперативные подразделения тесно контактируют с дежурными частями ОВД. Для выявления лиц и фактов, представляющих оперативный интерес, а также в раскрытии преступлений оперативные подразделения активно привлекают участковых уполномоченных полиции. При раскрытии преступлений, совершаемых несовершеннолетними, как правило, привлекаются сотрудники ПДН, от которых можно получить сведения о подростках, склонных к преступной деятельности. Эффективная работа по раскрытию краж и угонов автотранспортных средств невозможна без привлечения сил и средств сотрудников ГИБДД.



Много общих задач подразделениям уголовного розыска приходится решать с подразделениями ЭбиПК, поэтому их взаимодействие осуществляется в различных формах. В частности, совместное оперативное обслуживание криминогенных объектов позволяет устанавливать лиц и факты, представляющие оперативный интерес для обеих служб. Совместное осуществление оперативной отработки заподозренных и проверяемых лиц дает возможность наиболее полно разоблачать организованные преступные группы, чья противоправная деятельность носит одновременно и общеуголовную, и экономическую

направленность. Кроме того, раскрытие подразделениями уголовного розыска краж у юридических лиц может быть затруднительно без привлечения специалистов по борьбе с экономическими преступлениями.

Тесным образом должны взаимодействовать подразделения уголовного розыска территориальных и транспортных ОВД при выявлении и разоблачении преступников-гастролеров, раскрытии преступлений, совершаемых на сопредельной территории оперативного обслуживания, выявлении и пресечении незаконного оборота наркотиков, розыске скрывшихся преступников и лиц, пропавших без вести.



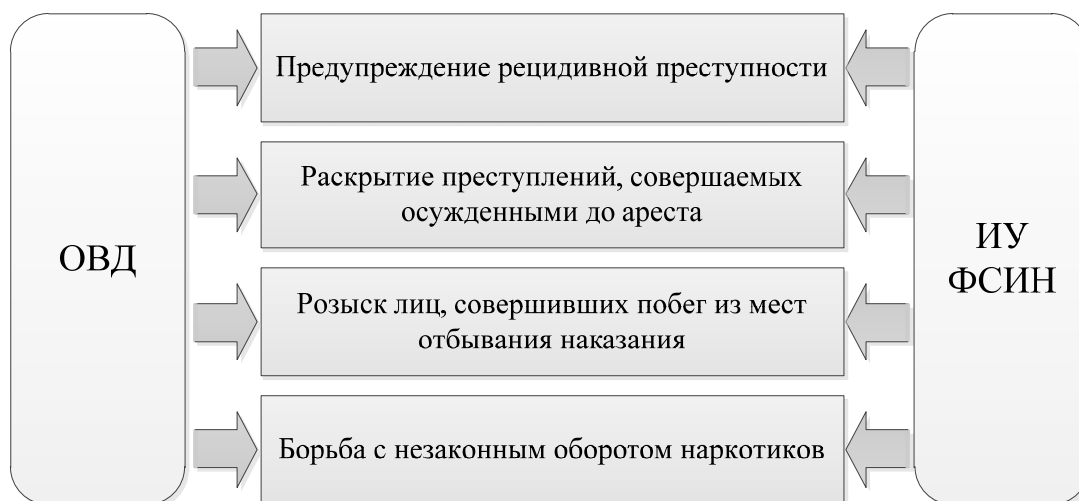
Взаимодействие и сотрудничество оперативных подразделений с другими субъектами оперативно-розыскной деятельности, государственными органами, уполномоченными на осуществление контрольной и надзорной деятельности в сфере ИКТ, и иными государственными органами

Необходимость взаимодействия оперативных подразделений ОВД с другими субъектами ОРД обусловлена большим разнообразием совместно решаемых задач. Например, при взаимодействии оперативных подразделений уголовного розыска с оперативными подразделениями исправительных учреждений ФСИН решаются следующие задачи:

- предупреждение рецидивной преступности;
- раскрытие преступлений, совершенных осужденными до ареста;
- розыск лиц, совершивших побег из мест лишения свободы.

Для решения этих задач оперативные подразделения ОВД должны регулярно направлять в оперативные подразделения исправительных учреждений ФСИН России информацию о нераскрытых преступлениях на территории оперативного обслуживания; о лицах, осужденных за преступления, не связанные с проводимой в отношении них негласной оперативной работы; о результатах проверки материалов, поступивших из мест лишения свободы о прошлой преступной деятельности осужденных.

В порядке взаимного обмена информацией из исправительных учреждений ФСИН России в оперативные подразделения ОВД направляются сведения о предстоящем освобождении воров в законе и лидеров уголовно-преступной среды; о лицах, намеревающихся после освобождения совершать преступления, а также потребляющих наркотики.



Скоординированная работа оперативных подразделений ОВД, ФСБ России и прокуратуры позволяет своевременно пресекать противоправную деятельность распространителей печатной продукции, фото-, аудио- и видеоматериалов (в том числе с использованием сети Интернет), направленных на пропаганду фашизма, возбуждение социальной, расовой, национальной ненависти и религиозной вражды; выявлять и пресекать незаконную, антиконституционную деятельность террористических, экстремистских и националистических группировок; выявлять и пресекать каналы финансирования этих структур.

Взаимодействие между оперативными подразделениями ОВД и ФСБ России осуществляется по самому широкому спектру вопросов, отнесенных к компетенции этих органов. В их числе: противодействие незаконному обороту наркотических средств, психотропных

веществ и их прекурсоров; противодействие незаконному обороту огнестрельного оружия, боеприпасов и взрывчатых веществ; проведение специальных операций по освобождению заложников; противодействие терроризму; обеспечение информационной безопасности Российской Федерации и борьба с преступлениями в сфере компьютерной информации; противодействие финансированию терроризма и экстремизма и т. д.

Одним из важнейших направлений сотрудничества органов МВД России и ФСБ России является согласованная совместная работа по выявлению, документированию и пресечению экстремистской деятельности иностранных граждан, лиц без гражданства, проживающих на территории России и подозреваемых в связях с зарубежными террористическими и экстремистскими центрами и организациями.

Особое место занимает взаимодействие оперативных подразделений ОВД с Федеральной службой по финансовому мониторингу (Росфинмониторингом). Одной из основных форм такого взаимодействия является информационный обмен, осуществляемый посредством направления письменных запросов и ответов на них. При наличии достаточных оснований, свидетельствующих о том, что операция (сделка) связана с легализацией (отмыванием) доходов, полученных преступным путем, или с финансированием терроризма, Росфинмониторинг направляет соответствующую информацию и материалы в правоохранительные органы в соответствии с их компетенцией. Поступившие от службы информация и материалы принимаются к производству оперативным подразделением, как правило, по территориальности совершения действий, вызывающих подозрение в легализации (отмывании) доходов, полученных преступным путем. В зависимости от значимости информации, а также межрегионального характера совершенного деяния материалы могут быть приняты к производству соответствующим оперативным подразделением Центрального аппарата МВД России или подразделениями ГУ МВД России по федеральным округам.

В случае принятия процессуального решения в порядке ст. 145 УПК РФ об этом информируется Федеральная служба по финансовому мониторингу.

Взаимодействие с подразделениями обеспечения безопасности банковских и иных финансовых подразделений, операторами связи, провайдерами и другими организациями, оказывающими услуги в сфере ИКТ

Порядок взаимодействия подразделений безопасности банковских и иных финансовых предприятий с оперативными подразделе-

ниями ОВД регламентируется Федеральными законами «Об ОРД», «О банках и банковской деятельности», другими НПА. В целях противодействия коррупции оперативные подразделения органов, осуществляющих ОРД, могут обращаться с соответствующими запросами в службу безопасности банка или иную финансовую организацию. Согласно Федеральному закону от 01.04.2022 № 77-ФЗ «О внесении изменений в статью 26 Федерального закона «О банках и банковской деятельности» и статью 9 Федерального закона «Об оперативно-розыскной деятельности» уточнен порядок представления кредитными организациями информации должностным лицам органов, уполномоченных осуществлять ОРД. Установлено, в частности, что справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, а также по операциям, счетам и вкладам физических лиц предоставляются кредитными организациями на основании судебного решения в течение 10 рабочих дней со дня получения соответствующего постановления.

Порядок взаимодействия операторов связи с органами, осуществляющими ОРД, регламентируется ФЗ «О связи» и ФЗ «Об ОРД». В соответствии с этими законами приняты следующие подзаконные акты: приказ Мининформсвязи России, ФСБ России от 15.01.2008 № 5/8 «Об утверждении Типовых требований к плану мероприятий по внедрению технических средств для проведения оперативно-розыскных мероприятий»; приказ Мининформсвязи России от 16.01.2008 № 6 «Об утверждении Требований к сетям электросвязи для проведения ОРМ. Часть I. Общие положения». Основным НПА, которым в своей повседневной деятельности руководствуются операторы связи и специальные службы, наделенные полномочиями по осуществлению ОРД, являются Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность¹. Данные Правила определяют порядок предоставления операторами связи уполномоченным органам информации об абонентах и оказанных им услугах связи, а также иной информации, необходимой для выполнения возложенных на уполномоченные органы задач в порядке и случаях, установленных федеральными законами. От имени уполномоченных органов взаимодействие с операторами связи возложено на УФСБ по субъекту РФ – местонахождению сети связи. Взаимодействие (сотрудничество)

¹ Утверждены постановлением Правительства РФ от 27.08.2005 № 538 (в ред. постановления Правительства РФ от 25.09.2018 г. № 1138).

ФСБ с операторами, предоставляющими услуги связи, осуществляется по следующим направлениям.

1. Лицензирование деятельности операторов по предоставлению населению услуг связи. На этом этапе осуществляются: разработка плана мероприятий по внедрению технических средств, его согласование и реализация; присоединение СПД к сети оператора, сдавшего технические средства специальных ОРМ в постоянную эксплуатацию; обслуживание технических средств для проведения ОРМ.

2. Предоставление оператором баз данных информации об абонентах, оказанных услугах связи (в том числе о соединениях, трафике и платежах абонентов). Информация предоставляется ФСБ путем осуществления круглосуточного удаленного доступа к базам данных и хранится в течение трех лет: сотрудники оперативно-технических подразделений ФСБ могут проводить онлайн мониторинг переговоров и контроль сообщений на расстоянии из пункта управления.

3. Предоставление технических средств специальных ОРМ, которые должны обеспечивать сбор информации о выделенных реальных IP-адресах, передаваемой информации, в том виде и последовательности, в которых такая информация поступала; о местоположении пользовательского оборудования.

Операторы связи должны следить за тем, чтобы абоненты сетей связи не могли по каким-либо признакам установить, прослушиваются их разговоры или нет. Не должно быть таких возможностей и у персонала компании связи. Защита от несанкционированного доступа сотрудников оператора связи к информации, относящейся к проведению ОРМ, является одним из обязательных требований к сетям электросвязи.

Участие операторов связи в ОРМ заключается не только в их обязанности содействовать органам, осуществляющим ОРД, но и в обязанности заботиться о необходимом техническом оснащении сетей связи для проведения ОРМ.

Примерный план занятия

1. Нормативная основа взаимодействия.
2. Понятие, виды и формы взаимодействия.
3. Взаимодействие оперативных подразделений с иными службами и подразделениями органов внутренних дел.
4. Взаимодействие и сотрудничество оперативных подразделений с другими субъектами оперативно-розыскной деятельности, государственными органами, уполномоченными на осуществление кон-

трольной и надзорной деятельности в сфере ИКТ, и иными государственными органами.

5. Взаимодействие с подразделениями обеспечения безопасности банковских и иных финансовых подразделений, с операторами связи, провайдерами и другими организациями, оказывающими услуги в сфере ИКТ.

Вопросы для самоконтроля по теме

1. Виды ведомственных нормативных правовых актов МВД России, определяющих организацию и тактику взаимодействия между различными службами и подразделениями ОВД.

2. Понятие взаимодействия.

3. Виды взаимодействия.

4. Формы взаимодействия.

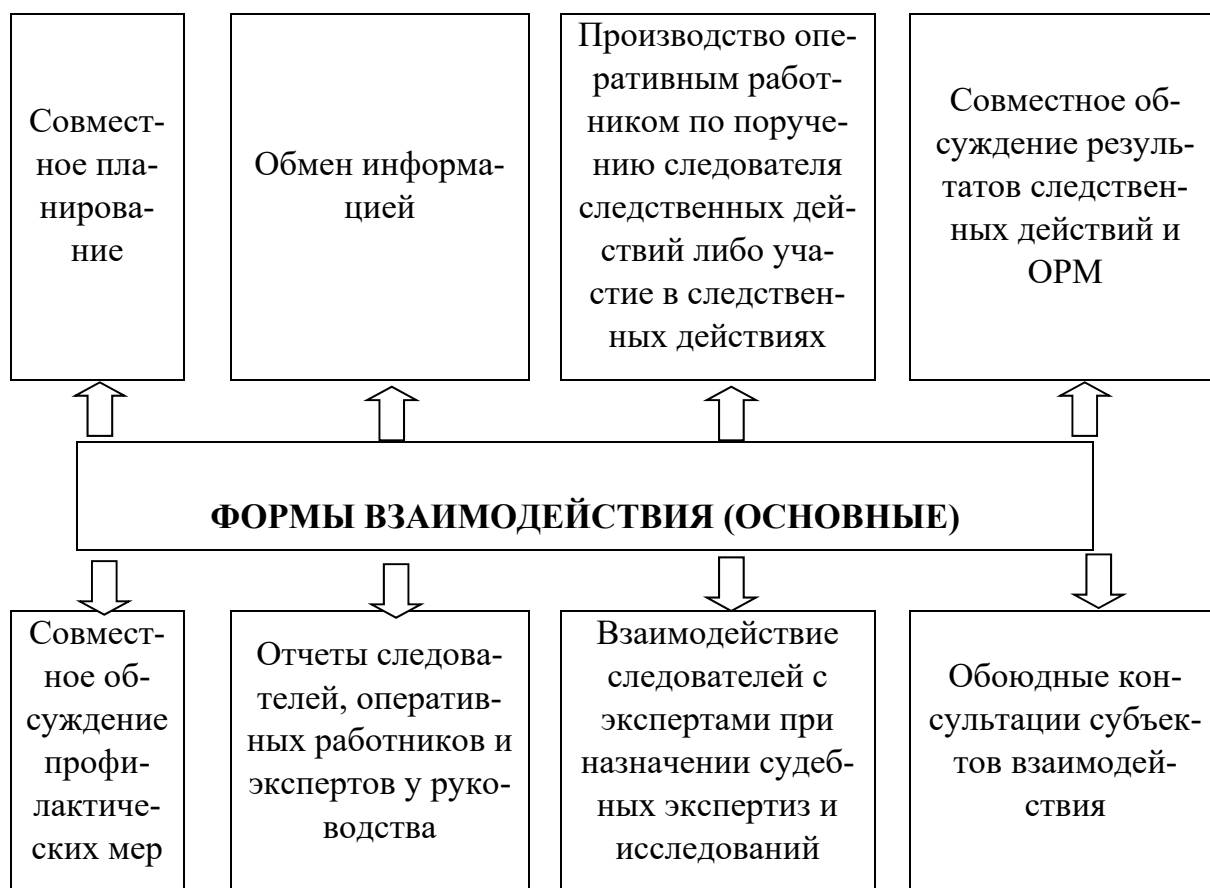
5. Субъекты взаимодействия.

Тема 2.14. Взаимодействие оперативных подразделений с органами предварительного следствия и дознания

В современных условиях раскрытия преступлений их полное и качественное расследование невозможно без согласованной, направленной на конечный результат работы органов предварительного следствия и оперативных служб. Под конечным результатом следует понимать реализацию главной функции правоохранительной системы – защиту конституционных прав граждан от преступных посягательств при безусловном соблюдении законности на всех этапах правоприменительного процесса.

В числе приоритетных задач, поставленных перед ОВД, обозначены задачи реализации исчерпывающих мер по активизации взаимодействия органов предварительного следствия, оперативных, экспертно-криминалистических подразделений, средств массовой информации и граждан в целях повышения результативности раскрытия и расследования преступлений, в том числе по которым не установлены лица, подлежащие привлечению в качестве обвиняемых. Укрепление и совершенствование взаимодействия является необходимым условием эффективности и результативности деятельности оперативных подразделений. Актуальность этой задачи вытекает из анализа оперативной обстановки, который в последние годы свидетельствует о постоянном увеличении количества преступлений, остающихся нераскрытыми.

Взаимодействие должно начинаться с момента получения оперативно значимой информации, заведения дела оперативного учета и продолжаться до стадии судебного разбирательства. Вопросы взаимодействия по выявлению, раскрытию и расследованию преступлений регулярно рассматриваются на заседании коллегии МВД России, оперативных совещаниях при Министерстве внутренних дел РФ и его заместителях.



Поскольку принятию решения о возбуждении уголовного дела предшествует целый комплекс проверочных мероприятий, то в ОВД, в связи со сложностью раскрытия отдельных категории преступлений, включая совершаемые с применением ИКТ, создаются **следственно-оперативные группы (СОГ)**, назначение которых состоит в объединении совместных усилий следователей (дознавателей) и сотрудников уголовного розыска в целях эффективного сочетания сил и средств правоохранительных органов для всестороннего и полного раскрытия и расследования преступлений.

Своевременно созданные СОГ, правильная организация их работы, взаимодействие подразделений дознания ОВД со следователями позволяют эффективно раскрывать многие преступления, реализуя непрерывность и неотложность следственных действий и ОРМ¹.

Эффективность взаимодействия при раскрытии преступлений определяется оперативным выездом на место происшествия, его квалифицированным осмотром, качественным использованием получен-

¹ Скогорева Т.Ф. и др. Организация взаимодействия при раскрытии и расследовании преступлений специализированными подразделениями дознания органов внутренних дел: учеб. пособие. Волгоград: ВА МВД России, 2016 С. 54.

ной информации, своевременным задействованием сил и средств соответствующих служб для осуществления розыскных мер, координацией и согласованием их деятельности, контролем за выполнением намеченных мероприятий.

В УПК РФ понятие СОГ не закреплено. Вопросы организации, структуры и деятельности СОГ регулируются ведомственными НПА. С учетом характера, объема и продолжительности решаемых задач СОГ имеют специфичные функции.

Дежурная СОГ (при дежурной части) создается для обеспечения производства неотложных следственных действий и ОРМ непосредственно после поступления сообщения о преступлении. Такая группа формируется в составе следователя или дознавателя (в зависимости от подследственности совершенного преступления), сотрудников оперативных подразделений, экспертно-криминалистических и иных подразделений, при необходимости – инспектора-кинолога. Эта группа формируется из числа сотрудников, осуществляющих дежурство в составе суточного наряда по ОВД¹.

Специализированная СОГ создается для обеспечения эффективного взаимодействия подразделений ОВД по конкретному уголовному делу. СОГ по рассматриваемой категории преступлений должна быть создана до возбуждения уголовного дела, поскольку требуется согласованная работа следователя (дознавателя) и сотрудников оперативных подразделений при поступлении информации о совершенном преступлении. Создание такой группы устраняет организационную разобщенность, способствует ведению одновременной, параллельной работы, в результате чего осуществляется постоянный взаимный обмен информацией между участниками СОГ.

Одним из принципов функционирования СОГ является разграничение компетенции следователя (дознавателя) и оперативных сотрудников. Координатором СОГ является следователь (дознаватель), однако выбор методов, сил и средств раскрытия преступления остается за оперативными сотрудниками, специализирующимися по разным направлениям деятельности².

¹ Скогорева Т.Ф. и др. Указ. соч. С. 57.

² См.: Фадеев И.А. Правовые основы организации взаимодействия следователя и оперативного сотрудника полиции // Российский следователь. 2014. № 4. С. 10–13.

Примерный план занятия

1. Правовая основа совместной деятельности оперативных и следственных подразделений.
2. Следственно-оперативные группы: понятие, виды и состав.
3. Деятельность сотрудников оперативных подразделений в составе следственно-оперативных групп и их полномочия как членов следственно-оперативной группы.

Вопросы для самоконтроля по теме

1. Виды следственно-оперативных групп.
2. Формы взаимодействия оперативных и следственных подразделений.
3. Полномочия сотрудников оперативных подразделений в составе следственно-оперативных групп.

Тема 2.15. Контроль и надзор за оперативно-розыскной деятельностью

Специфика использования сил, средств и методов ОРД, связанная с применением их в основном негласным способом, а также необходимость проведения ОРМ, ограничивающих конституционные права граждан, требует особого контроля за ее осуществлением со стороны различных институтов государственной власти.

В соответствии со ст. 20–22 ФЗ «Об ОРД» контроль за ОРД осуществляют Президент РФ, Федеральное Собрание и Правительство РФ в пределах полномочий, определяемых Конституцией РФ, федеральными конституционными и федеральными законами. Контроль со стороны руководителей органов, осуществляющих ОРД, заключается в том, что они несут персональную ответственность за соблюдение законности при организации и проведении ОРМ. Прокурорский надзор за исполнением ФЗ «Об ОРД» осуществляют Генеральный прокурор РФ и уполномоченные им прокуроры.

Контроль и надзор за ОРД обеспечивается:

- соблюдением законности и конституционных прав и свобод человека и гражданина в ОРД;
- независимостью при исполнении служебных обязанностей, исключением вмешательства третьих лиц и организаций в процесс проведения ОРМ;
- подотчетностью и подконтрольностью должностных лиц органов, осуществляющих ОРД;
- персональной ответственностью должностных лиц и руководителей оперативных подразделений за законность при осуществлении ОРМ.

Президентский контроль за ОРД

Контроль за ОРД Президентом Российской Федерации определен ст. 20 ФЗ «Об ОРД». Президент РФ, осуществляя свои полномочия высшего должностного лица государства, контролирует полноту и эффективность исполнения ФЗ «Об ОРД» на территории России, состояние подзаконной нормативной базы и соответствие ее действующему законодательству, общий уровень профессионализма субъектов ОРД и др.

Контроль за ОРД Президент РФ осуществляет через Главное контрольное управление, которое призвано проверять исполнение федеральных законов всеми органами исполнительной власти и должностными лицами.

В связи с тем, что силовые министерства и ведомства государства, включая МВД России, напрямую подчинены Президенту, это предполагает его контроль за деятельностью органов, осуществляющих ОРД, выражающийся:

- в заседаниях Правительства РФ, где рассматриваются вопросы, относящиеся к проведению спецопераций по борьбе с терроризмом (им заслушиваются руководители этих ведомств);

- в требованиях от должностных лиц правоохранительных ведомств объяснений, необходимых документов, другой информации, касающихся совершенствования ОРД и обеспечения правопорядка в обществе;

- в направлении предписаний на устранение выявленных нарушений руководителям органов, осуществляющих ОРД, привлечении виновных к ответственности;

- в осуществлении нормотворческой деятельности: принятии указов по вопросам совершенствования ОРД, например: от 1 сентября 1995 г. № 891 «Об упорядочении организации и проведения ОРМ с использованием технических средств», от 18 апреля 1996 г. № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью» и др.

Правительственный контроль за ОРД

В соответствии со ст. 114 Конституции РФ Правительство РФ осуществляет меры по обеспечению законности, прав и свобод граждан, охране собственности и общественного порядка, борьбе с преступностью. Членами Правительства РФ являются Министр внутренних дел РФ, директор Федеральной службы безопасности и другие руководители, которые организуют и контролируют ОРД.

В процессе контроля Правительство РФ проверяет полноту, законность и эффективность использования министерствами и ведомствами предоставленных им полномочий по осуществлению ОРД.

Одним из направлений контрольной деятельности Правительства РФ является проверка соответствия ведомственных НПА, регламентирующих ОРД, Конституции РФ и федеральному законодательству и обладание полномочиями их отмены в случае противоречия закону.

Другим направлением контроля за ОРД со стороны Правительства РФ является совещание членов Правительства РФ по вопросам обеспечения правопорядка, охраны собственности и безопасности граждан от преступных посягательств, в ходе которого заслушиваются отчеты о состоянии ОРД по борьбе с преступностью.

Парламентский контроль за ОРД

Федеральное Собрание – парламент РФ с соответствии со ст. 20 ФЗ «Об ОРД» наделен правом контролировать ОРД.

Парламентский контроль за ОРД могут осуществлять как отдельные комитеты Государственной Думы (по безопасности, по законодательству и судебно-правовой реформе и др.), так и аналогичные комитеты Совета Федерации.

Парламентский контроль осуществляется в форме парламентских слушаний и расследований, а также отчетов и сообщений должностных лиц соответствующих государственных органов в палатах Федерального Собрания.

Парламентский контроль может проводиться по двум основным направлениям: за расходованием выделяемых финансовых средств на осуществление ОРД и, собственно, за осуществлением ОРД по следующим направлениям:

- соблюдение прав и свобод человека и гражданина;
- соответствие ведомственных НПА, касающихся ОРД, действующему законодательству;
- кадровая политика органов, осуществляющих ОРД.

Парламентский контроль за ОРД допускается до определенных пределов. Так, финансовый контроль может проводиться только за обоснованностью выделения средств, а также за правильностью и эффективностью их использования.

Контроль за соблюдением прав и свобод человека и гражданина может проводиться в порядке парламентских расследований фактов нарушений прав и свобод человека и гражданина.

Контроль кадровой политики не опускается ниже уровня назначения руководителей самостоятельных подразделений центральных аппаратов государственных органов, осуществляющих ОРД, а также назначения руководителей таких органов в республиках и иных субъектах РФ.

Конституционный контроль за ОРД органов внутренних дел – особый вид правоохранительной деятельности, заключающийся в проверке соответствия законов и иных НПА Конституции РФ. В Российской Федерации такой контроль осуществляется Конституционным судом РФ, который самостоятельно и независимо осуществляет судебную власть посредством конституционного судопроизводства.

Полномочия и порядок деятельности Конституционного суда РФ определяются Конституцией РФ и Федеральным конституционным законом от 21 июля 1994 г. №1-ФКЗ «О Конституционном суде

Российской Федерации». В соответствии с ч. 4 ст. 125 Конституции РФ Конституционный Суд РФ по жалобам на нарушение конституционных прав и свобод граждан и запросам судов проверяет конституционность закона, примененного или подлежащего применению в рассматриваемом деле.

Поводом к рассмотрению дела является обращение в Конституционный суд РФ в форме запроса, ходатайства или жалобы. Основанием к рассмотрению дела является обнаружившаяся неопределенность в соответствии Конституции РФ оспариваемого НПА. Правом на обращение в Конституционный суд РФ с индивидуальной (коллективной) жалобой на нарушение конституционных прав и свобод обладают граждане и иные лица (объединения граждан, органы, организации, указанные в ФКЗ), чьи права и свободы нарушаются законом, примененным в конкретном деле. С конституционной жалобой могут обратиться не только российские, но и иностранные граждане, а также лица без гражданства. Жалоба граждан на нарушение законом конституционных прав и свобод признается допустимой при соблюдении трех основных условий: 1) закон затрагивает конституционные права и свободы; 2) имеется документальное подтверждение применения закона в конкретном деле; 3) рассмотрение дела должно быть завершено в суде. По запросам судов Конституционный суд РФ проверяет конституционность закона, подлежащего применению в конкретном деле, находящемся в производстве суда.

Судебный контроль за ОРД органов внутренних дел – деятельность суда по проверке решений и действий должностных лиц ОВД, осуществляющих ОРД, на соответствие требованиям ФЗ «Об ОРД» в целях определения законности и обоснованности решения процессуально-правовых вопросов, т. е. создания условий для надлежащего отправления правосудия и защиты прав и законных интересов человека и гражданина.

Субъекты судебного контроля за ОРД	
Суды первой инстанции	Районные и гарнизонные военные суды
Суды второй инстанции	Верховные суды республик, краевые, областные суды, суды городов федерального значения, суды автономных областей и автономных округов, окружные (флотские) военные суды
Суд третьей инстанции	Верховный Суд Российской Федерации

Основные цели судебного контроля за ОРД:

1) соблюдение прав и законных интересов человека и гражданина при осуществлении ОРД;

2) выявление фактов нарушения законности, допущенных в ходе ОРД, и привлечение к ответственности лиц, допустивших эти нарушения.

Формы судебного контроля за ОРД	
Предварительный судебный контроль	Осуществляется на этапе рассмотрения вопроса о возможности проведения ОРМ, ограничивающих конституционные права граждан
Ревизионный судебный контроль	Осуществляется после завершения ОРМ в отношении конкретного лица по жалобе и заявлению указанного лица на действия органов, осуществляющих ОРД

Прокурорский надзор за ОРД органов внутренних дел осуществляет строго очерченный законом круг субъектов – уполномоченные прокуроры, а объект и предмет надзора отнесены законом к разряду государственной тайны.

Правовой основой определения предмета прокурорского надзора в сфере ОРД являются Федеральные законы «Об ОРД», от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации» (далее – ФЗ «О прокуратуре РФ»), межведомственные и ведомственные НПА.

Полномочия прокурора по надзору за ОРД полиции определены ФЗ «О прокуратуре РФ», ФЗ «Об ОРД», указанием Генпрокуратуры России и МВД России от 29 сентября 2008 г. № 215/69, 1/7818.

Согласно положениям ст. 22 ФЗ «О прокуратуре РФ» прокурор при осуществлении возложенных на него функций вправе:

- по предъявлении служебного удостоверения беспрепятственно входить на территории и в помещения органов полиции, иметь доступ к их документам и материалам, проверять исполнение законов в связи с поступившей в органы прокуратуры информацией о фактах нарушения закона;

- требовать от руководителей и других должностных лиц представления необходимых документов, материалов, статистических и иных сведений; выделения специалистов для выяснения возникших вопросов; проведения проверок по поступившим в органы прокуратуры материалам и обращениям, ревизий деятельности подконтрольных или подведомственных им организаций;

- вызывать должностных лиц и граждан для объяснения по поводу нарушения законов;

- по основаниям, установленным законом, возбуждать производство об административном правонарушении, требовать привлечения лиц, нарушивших закон, к иной установленной законом ответственности, предостерегать о недопустимости нарушения закона;
- освобождать своим постановлением лиц, незаконно подвергнутых административному задержанию на основании решений несудебных органов;
- опротестовывать противоречащие закону правовые акты, обращаться в суд или арбитражный суд с требованием о признании таких актов недействительными;
- вносить представление об устранении нарушений закона.

Прокурор имеет право проверять исполнение законов только в связи с поступившей в органы прокуратуры информацией о фактах нарушения закона. Различные плановые и инициативные прокурорские проверки не имеют под собой правовой базы.

Ведомственный контроль в органах внутренних дел за ОРД

В соответствии со ст. 22 ФЗ «Об ОРД» и ст. 49 ФЗ «О полиции» ведомственный контроль за ОРД в целях своевременного, полного и эффективного принятия мер по решению задач ОРД, обеспечения соблюдения прав и законных интересов граждан, рационального и эффективного расходования финансовых средств осуществляют руководители ОВД, уполномоченных на осуществление ОРД.

В соответствии с приказом МВД России от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России» правом контроля за ОРД обладают следующие руководители органов внутренних дел:

- 1) в центральном аппарате МВД России:
 - министр внутренних дел РФ и его заместители, ответственные за деятельность оперативных подразделений;
 - начальники Главного управления уголовного розыска, Главного управления экономической безопасности и противодействия коррупции, Главного управления по противодействию экстремизму, Главного управления собственной безопасности, Главного управления на транспорте, Национального центрального бюро Интерпола, Управления по обеспечению безопасности лиц, подлежащих государственной защите, Управления оперативно-розыскной информации МВД России и их заместители;
- 2) в территориальных органах МВД России:
 - начальники территориальных органов МВД России и их заместители, ответственные за деятельность подразделений, осуществляющих ОРД, заместители начальников полиции по оперативной работе;

– начальники подразделений уголовного розыска, экономической безопасности и противодействия коррупции, по борьбе с преступными посягательствами на грузы, собственной безопасности, оперативно-розыскной информации, по противодействию экстремизму, по обеспечению безопасности лиц, подлежащих государственной защите, бюро специальных технических мероприятий, оперативно-поисковых бюро, межрегиональных оперативно-розыскных подразделений, оперативно-розыскных частей территориальных органов МВД России, за исключением территориальных органов МВД России на районном уровне;

– начальники отделов (отделений, пунктов) полиции в составе территориальных органов МВД России на межрегиональном и районном уровнях и их заместители, ответственные за деятельность подразделений, осуществляющих ОРД, при наличии штатных должностей оперативных сотрудников.

Основными целями ведомственного контроля за ОРД являются:

- 1) соблюдение прав и законных интересов человека и гражданина при осуществлении ОРД;
- 2) эффективное и правильное решение вопросов организации и тактики ОРД и своевременное устранение выявленных недостатков;
- 3) выявление фактов нарушения законности и правил конспирации, допущенных в ходе ОРД, и привлечение к ответственности лиц, допустивших эти нарушения.

Примерный план занятия

1. Цель, задачи и назначение контроля за ОРД.
2. Субъекты контроля за ОРД, их права и сфера деятельности.
3. Виды контроля за ОРД. Назначение и формы судебного контроля.
4. Понятие и сущность прокурорского надзора за ОРД.
5. Предмет прокурорского надзора за ОРД, организация и порядок его осуществления.

Вопросы для самоконтроля по теме

1. Назовите виды контроля за ОРД.
2. Основные цели судебного контроля за оперативно-розыскной деятельностью.
3. Полномочия прокурора по надзору за оперативно-розыскной деятельностью.
4. Основные цели ведомственного контроля за оперативно-розыскной деятельностью.

Перечень нормативных правовых актов, основной и дополнительной учебной литературы

Нормативные правовые акты

1. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.): ратифицировано Россией в 2008 году: Федеральный закон «О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 01.10.2008 № 164-ФЗ.

2. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ // Рос. газ. 2006. 29 июля.

3. О связи: федер. закон от 07.07.2003 г. № 126-ФЗ // Рос. газ. 2003. 10 июля.

4. Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность: постановление Правительства РФ от 27.08.2005 № 538 (в ред. от 25.09.2018 № 1138). Доступ из справ.-правовой системы «КонсультантПлюс».

5. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД РФ: приказ МВД России от 19.07.2012 № 608. Документ опубликован не был.

6. Приказ МВД России от 29.04.2015 № 495 дсп. Документ опубликован не был.

7. Приказ МВД России, МО России, ФСБ России, ФСО России, ФТС, СВР России, ФСИН России, ФСКН России, СК России от 27 сентября 2013 № 776/703/509/507/1820/42/535/398/68. Документ опубликован не был.

8. Государственный стандарт Российской Федерации «Делопротоизводство и архивное дело. Термины и определения». ГОСТ Р 51141-98: принят и введен в действие постановлением Госстандарта России от 27.02.1998 № 28.

Основная литература

1. Гаврилин Ю.В., Головин А.Ю., Тишутина И.В. Криминалистика в понятиях и терминах: учеб, пособие / под ред. А.Ю. Головина. М., 2006.

2. Дубоносов Е.С. Оперативно-розыскная деятельность: учеб. для вузов. М., 2013.

3. Маркушин А.Г. Оперативно-розыскная деятельность: учеб. для вузов. М., 2012.

4. Мулукаев Р.С., Хоботов А.Н., Суслов В.М. Становление и развитие аппаратов уголовного розыска в России (1917–1934 гг.): учеб. пособие. М.: МЮИ МВД России, 1994.

5. Основы оперативно-розыскной деятельности: учеб. / под ред. В.Б. Рушайло. СПб., 2000.

6. Оперативно-розыскная деятельность: учеб. / под ред. К.К. Горяинова, В.С. Овчинского, А.Ю. Шумилова. М.: ИНФРА-М, 2001.

7. Основы оперативно-розыскной деятельности органов внутренних дел: учебник / под общ. ред. Ю.А. Агафонова, Ю.Ф. Кваши. Краснодар: Кру МВД РФ. 2008.

8. Попов В.Л. Теоретико-правовые аспекты проблемы совершенствования оперативно-розыскной деятельности. Калининград: Калининградский юрид. ин-т МВД России, 1998.

Дополнительная литература

1. Компьютерная система – это набор аппаратных средств и периферийных устройств, составляющих в совокупности вычислительную машину: Справочник технического переводчика. URL: https://technical_translator_dictionary.academic.ru/93704

3. ОБЩИЕ ПОЛОЖЕНИЯ ПО РАССЛЕДОВАНИЮ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Тема 3.1. Действия сотрудников органов внутренних дел при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием информационно- коммуникационных технологий

Действия сотрудников ОВД при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием ИКТ, зависят от способа совершения противоправного деяния. Как правило, это дистанционные мошенничества, совершенные посредством телефонного звонка или интернет-ресурсов, или хищения денежных средств с использованием вредоносного ПО.

Наиболее распространенными по способу совершения являются *дистанционные мошенничества, совершенные посредством телефонного звонка* с различными преступными фабулами.

Например, заявителю посредством телефонного звонка от лица родственника или знакомого сообщают о том, что он задержан сотрудниками полиции за совершение того или иного преступления или правонарушения (ДТП, хранение оружия или наркотиков, причинение вреда здоровью), но есть возможность за определенное вознаграждение решить вопрос. Далее в разговор вступает другое лицо, которое представляется сотрудником правоохранительных органов и сообщает: какую сумму, куда и каким образом необходимо перечислить. Например, денежные средства могут быть переданы заявителем курьеру (таксисту), перечислены безадресным переводом, на банковский счет (электронный кошелек) или на лицевой счет абонентского номера телефона.

При получении сообщения о таком преступлении сотруднику ОВД необходимо у лица, обратившегося с заявлением, выяснить следующую информацию, отразив ее в объяснении:

- 1) дата, время поступления звонка с соответствующим содержанием;
- 2) абонентский номер заявителя, на который был осуществлен звонок (стационарный, мобильный телефон);

– если звонок поступил на сотовый телефон или стационарный телефон с автоматическим определением номера, с какого номера телефона осуществлен звонок;

3) дословное содержание разговора (кем представился звонивший, о чем говорил, что предлагал сделать и др.);

4) описание голоса и особенностей речи звонившего, по которым его можно опознать:

– дефекты речи: хрипота, картавость, шепелявость, заикание и т. д.;

– громкость голоса: пониженный тон, повышенный тон, обычный тон, громкий шепот, приглушенное звучание и т. п., попытки изменить естественный тембр голоса;

– особенности интонации, произношения отдельных звуков, в том числе, региональные;

– использование в разговоре особенных фразеологизмов: специфических речевых оборотов, специальных терминов, диалектизмов;

– употребление «слов-паразитов», избыточных междометий;

– темп речи, характерность пауз;

5) качество связи: помехи, ухудшение или прерывание слышимости и др.;

6) содержание (по возможности дословное) сообщение самого заявителя неизвестным, представившимся родственником и сотрудником полиции;

7) обстоятельства получения неизвестным точного адреса места жительства заявителя: последний сам его назвал либо неизвестный, представившийся сотрудником полиции, уже знал этот адрес;

8) продолжительность телефонного разговора с неизвестным (для сверки в последующем с данными детализации телефонных переговоров);

9) период времени после окончания разговора, через который неизвестный звонивший подъехал к дому заявителя;

10) описание голоса и особенностей речи неизвестного лица (курьера, таксиста), пригодные для опознания заявителем (см. п. 4);

11) подробное описание внешности «курьера» («таксиста»): черт лица, рук, особенностей телосложения, а также походки, поведения, одежды по которым заявитель сможет его опознать (композиционный портрет личности);

12) если передача денег осуществлялась в жилище заявителя, установить: до каких предметов мебели, интерьера иных предметов дотрагивался «курьер» («таксист») в помещении, как себя вел;

13) содержание разговора с «курьером» («таксистом»): что тот сообщил, задавал ли какие-либо вопросы, задавал ли заявитель ему какие-либо вопросы, интересовался ли судьбой своего родственника, например, путем постановки вопроса, когда родственника освободят от уголовной ответственности и пр.;

14) сообщал ли заявитель неизвестному точную сумму денег, которую передал ему, для каких целей он передает ему эти деньги;

15) судя по поведению неизвестного, был ли тот осведомлен о содержимом переданном ему, о причинах (целях) передачи ему денежных средств;

16) пересчитывали ли заявитель или неизвестное лицо деньги на месте их передачи;

17) как заявитель упаковал деньги;

18) звонил ли неизвестный в момент получения денег кому-либо, содержание этого сообщения или части диалога;

19) провожал ли заявитель неизвестного, наблюдал ли за направлением, в котором неизвестный покинул место расположения его дома, передвигался ли неизвестный на автомобиле (какой модели);

20) какую сумму денег заявитель хранит дома;

21) как часто заявителя посещает родственник, якобы попавший в беду, как заявитель может охарактеризовать его: характер их взаимоотношений, трудовой деятельности родственника и источников его доходов, наличие в кругу общения родственника лиц, ранее привлеченных к уголовной ответственности, отбывших наказание, в частности, в местах лишения свободы;

22) кто из посторонних лиц посещает или посещал в последнее время заявителя (социальный работник, медицинский работник, представитель организации по вопросам пенсионного обеспечения и пр.), его полные анкетные данные, контактные номера телефонов, характеристика его заявителем, частота посещений, последняя дата посещения; знаком ли посетитель (медицинский работник) с родственником заявителя, якобы попавшим в беду, знает ли социальный работник, где проживает родственник, якобы попавший в беду.

При осуществлении безадресного перевода, необходимо выяснить, на чье имя переводились деньги, полные установочные данные получателя, истребовать у заявителя квитанцию о переводе. Если перевод был осуществлен на лицевой счет абонентского номера или счет банковской карты, необходимо выяснить:

а) абонентский номер телефона или номер банковской карты, с которой переведены денежные средства (дата получения, срок дей-

ствия, вид платежной системы, банк-эмитент карты, наличие договора банковского счета и документов об оформлении банковской карты), истребовать данные документы, чек или квитанцию о переводе;

б) абонентский номер телефона или номер банковской карты, на которую переведены денежные средства;

в) размер суммы перевода денежных средств;

г) предпринятые заявителем действия после обнаружения факта мошеннических действий;

д) значительность ущерба для заявителя; если да, то обязательно отразить обстоятельства, подтверждающие это: состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Далее с помощью сайта Федерального агентства связи «Россвязь» по ссылке: http://rossvyaz.ru/activity/num_resurs/registerNum или www.kody.ru на вкладке «Коды сотовых операторов» или иных сайтах необходимо установить принадлежность оператору и региону абонентских номеров, использовавшихся при совершении мошенничества.

Затем устанавливаются анкетные данные владельца абонентского номера, который использовался при совершении преступления. Для этого направляется запрос в БСТМ УМВД России по региону (краю или области) с указанием необходимости обращения к соответствующему оператору сотовой связи за предоставлением сведений о пользователе услуги связи: Ф.И.О. абонента, дата рождения, адрес регистрации, паспортные данные. Следует обратить внимание, что в случае если абонентский номер входит в номерную емкость оператора связи за пределами региона инициатора запроса, то направляется запрос за подписью руководителя территориального органа МВД России на районном уровне в ПСТМ территориального органа МВД России по интересующему субъекту Российской Федерации.

В дальнейшем применяются меры по подготовке постановления о возбуждении ходатайства перед судом о получении разрешения на проведение ОРМ «Наведение справок» (ОРМ «Снятие информации с технических каналов связи», ограничивает конституционные права человека и проводится ПСТМ только по заданиям в рамках дел оперативного учета) с целью получения информации о соединениях абонентских номеров, используемых при совершении преступления, с указанием местонахождения базовых станций и IMEI телефонных аппаратов, в которых использовались абонентские номера, получение сведений об изменении баланса лицевого счета абонентских номе-

ров, а также статистики соединений установленных IMEI телефонных аппаратов с указанием базовых станций. Необходимо помнить, что данное мероприятие может быть выполнено только сотрудником уголовного розыска.

Соответствующим запросом направляется постановление суда в ПСТМ территориального органа МВД России по субъекту, на территории которого оказывает услуги связи интересующий оператор связи.

В зависимости от движения похищенных в результате мошенничества денежных средств (в том числе, при переводе с лицевого счета абонентского номера, на который переводил заявитель, на счет банковской карты, платежной системы) готовится постановление о возбуждении ходатайства перед судом в соответствии с ч. 5 ст. 26 Федерального закона «О банках и банковской деятельности».

Постановление суда вместе с соответствующим запросом направляется в банк, выпустивший карту¹ (банк можно определить по первым 6 цифрам, указанным в номере банковской карты. Данную информацию можно получить, перейдя по ссылке: <https://www.bindb.com/bin-database.html>

При переводе похищенных денежных средств на электронные кошельки одной (любой) из платежных систем подготавливается аналогичное постановление о возбуждении ходатайства перед судом в соответствии с ч. 5 ст. 26 Федерального закона «О банках и банковской деятельности».

Соответствующим запросом направляется постановление суда в администрацию платежных систем с указанием о необходимости сообщения сведений об IP-адресах регистрации и использования с указанием времени, а также движении по нему денежных средств с указанием расчетных счетов и номеров банковских карт получателей в интересующий период².

Алгоритм действий сотрудника ОВД при получении заявления (сообщения) о дистанционном мошенничестве, совершенном с использованием сети Интернет. Как правило, такие преступления связаны с размещением объявлений в сети Интернет, посредством которых происходит обман граждан.

¹ При подготовке постановлений и запросов необходимо иметь в виду, что номер банковской карты не совпадает с номером расчетного счета, к которому она привязана.

² Юридические адреса и реквизиты платежных систем указаны на официальных сайтах в сети Интернет.

Как и в предыдущем случае, сотрудник полиции должен установить обстоятельства совершенного преступления, указывающие на объективное подтверждение факта противоправного деяния. Такими обстоятельствами, как указано выше, является информация о времени совершения преступления, месте, способе, лицах и причиненном ущербе.

Первоначально необходимо получить объяснение от лица, в отношении которого совершено противоправное деяние, в ходе которого выяснить следующие обстоятельства:

1) дату и время обнаружения объявления (получения ссылки на соответствующий интернет-ресурс); если возможно, найти объявление в Интернете и зафиксировать его адрес (еще раз пройти по интернет-ссылке), сделать снимок экрана, приобщить его к материалам проводимой проверки;

2) техническое устройство, через которое заявитель выходил на сайт с размещенным объявлением (переходил по интернет-ссылке): стационарный компьютер, мобильное устройство;

3) характеристики товара, указанные в объявлении о продаже;

4) условия купли-продажи в объявлении: условия предоплаты, оплаты товара, сроки и виды поставки, ответственность сторон;

5) контактные данные продавца в объявлении о продаже;

6) наличие и характер отзывов, комментариев к объявлению о продаже;

7) сохранились ли у покупателя данные объявления (№ объявления, ID страницы);

8) каким образом, когда (дата, время) заявитель связался с продавцом;

9) как продавец представился;

10) где, со слов продавца, он находился;

11) известно ли ему место нахождения товара;

12) подробное содержание разговора с продавцом: что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю товара;

13) описание голоса и особенностей речи продавца, дающих возможность его опознания;

14) когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере заявитель перечислил на какой счет (№ счета, либо банковской карты, открытые на чье имя) денежные средства в счет оплаты за якобы приобретаемый товар;

15) если заявитель осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через «Личный кабинет» установить место входа 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 этот день заявителю услуги доступа в Интернет);

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

17) способ извещения потерпевшим «продавца» о перечислении денежных средств на указанную им банковскую карту (электронный кошелек);

18) содержание сообщения «продавца» потерпевшему после подтверждения оплаты (перечисления денег на банковскую карту «продавца»);

19) место и время прибытия для получения приобретенного товара;

20) время и обстоятельства осознания потерпевшим, что в отношении него было совершено мошенничество;

21) предпринятые заявителем действия после обнаружения факта мошеннических действий;

22) значительность ущерба для заявителя; если да, то обязательно отразить обстоятельства, подтверждающие это: состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

В ходе дальнейших мероприятий следует установить принадлежность доменного имени, адресов электронной почты, анкетные данные владельца абонентского номера, которые использовались при совершении преступления, для этого направить запрос в БСТМ УМВД России по региону с указанием необходимости предоставления сведений о принадлежности конкретного доменного имени, электронного почтового ящика, а также обращения к соответствующему оператору сотовой связи за предоставлением сведений о пользователе услугами связи: Ф.И.О. абонента, дата рождения, адрес регистрации, паспортные данные, копия договора об оказании услуг связи с указанием даты его заключения и расторжения.

В случае использования для совершения дистанционного мошенничества электронных торговых площадок, например Avito.ru, следует направить запрос владельцу данного сайта (в данном случае –

ООО «КЕХ еКоммерц») и иным торговым площадкам на предоставление сведений об IP-адресе размещения объявления с указанием даты и времени, контактных данных, указанных при регистрации на сайте, а также наличие жалоб на данное объявление.

При использовании социальных сетей необходимо направить запрос администратору социальной сети на предоставление сведений об IP-адресах регистрации и использования учетной записи, контактных данных, указанных при регистрации, об учетных записях, зарегистрированных с использованием интересующего абонентского номера (электронного почтового ящика).

При установлении IP-адреса лица, подозреваемого в совершении преступления при выходе в сеть Интернет и регистрации на различных ресурсах, нужно направить запрос в БСТМ УМВД России по региону с указанием необходимости обращения к соответствующему оператору сотовой связи за предоставлением сведений о пользователе услугами связи, а именно:

- кому предоставлена услуга доступа к сети Интернет и иные данные, связанные с услугами Интернета;
- геолокация данного лица, т. е. населенный пункт и конкретный адрес точки доступа;
- копия заключенного договора об оказании услуги;
- контактные данные лица, с которым заключен договор, а при наличии – и копии документов, удостоверяющих его личность.

Если общение происходило с использованием абонентского номера или он был указан как контактный, необходимо подготовить постановление о возбуждении ходатайства перед судом о получении разрешения на проведение ОРМ «Наведение справок» с целью получения информации о соединениях абонентского номера с указанием местонахождения базовых станций и IMEI телефонного аппарата, в котором использовался абонентский номер, статистики соединений установленного IMEI телефонного аппарата с указанием базовых станций.

При получении судебного постановления следует направить соответствующий запрос за подписью руководителя территориального органа МВД России на районном уровне в ПСТМ территориального органа МВД России по соответствующему субъекту Российской Федерации, на территории которого оказывает услуги связи интересующий оператор связи.

В зависимости от движения похищенных в результате мошенничества денежных средств готовится постановление о ходатайстве

перед судом о разрешении проведения ОРМ «Наведение справок», направленное на получение от кредитной организации справки по счету карты (счета юридического лица, электронному кошельку и т. д.), в соответствии с ч. 5 ст. 26 ФЗ «О банках и банковской деятельности». В резолютивной части постановления следует указать на необходимость предоставления кредитной организацией информации:

- о владельце банковской карты (счета юридического лица) и подключенных абонентских номерах к системе дистанционного банковского обслуживания;

- о движении денежных средств с указанием устройств самообслуживания (банкоматов), в которых производилось снятие денежных средств;

- о реквизитах платежных средств, с которых осуществлялось зачисление денежных средств, перевод;

- о СМС-распоряжениях, направленных в банк с мобильных устройств при помощи системы дистанционного банковского обслуживания (мобильный банк);

- об IP-адресах, дате, времени, с которых осуществлялся доступ и управление системой дистанционного банковского обслуживания (например, «Сбербанк-Онлайн»).

Полученное постановление суда с соответствующим запросом направляется в кредитную организацию.

Проведение мероприятий по факту хищения денежных средств с использованием вредоносного ПО

Опрос лица, которому причинен вред, включает в себя примерный перечень вопросов:

- 1) время, место и обстоятельства хищения денежных средств;

- 2) реквизиты банковской карты, с которой совершено хищение денежных средств, а также подключенной услуги «Мобильный банк» с указанием номеров телефонов, к которым она привязана;

- 3) если услуга подключена самим заявителем, то с какого времени и каким способом (посредством заявления о подключении в офисах банковских учреждений или посредством банкоматов);

- 4) с какого времени заявитель пользуется абонентским номером, к которому данная услуга подключена, так как не исключается невыпуск номера оператором связи после истечения 6 месяцев неиспользования абонентского номера с оформлением номера на иное лицо;

- 5) модель телефона, подключенного к услуге «Мобильный банк», используемая операционная система в телефоне («Андроид», IOS (Apple) или иное);

- 6) наличие антивирусных программ на мобильном устройстве;
- 7) какие мобильные приложения устанавливались в последнее время, способ установки (из официальных источников (сайтов) AppStore (Apple), PlayMarket (GooglePlay), с сайта банка-эмитента банковской карты (банковского продукта, в случае, например, открытия банковского счета без выпуска банковской карты);
- 8) совершались ли операции через мобильное устройство (телефон, планшет) или компьютер, вводились ли иным способом данные карты или хранились сведения о ней в устройствах;
- 9) осуществлялся ли с данного устройства доступ в сеть Интернет, в том числе автоматически (например, при установке графика автоматического обновления приложений) и каких именно приложений и пр.;
- 10) осуществлял ли кто-либо с использованием данных банковской карты (номера, срока действия, данных владельца, SVC/CVV2-кода (три цифры, расположенные на обратной стороне банковской карты) заявителя покупку товаров, заказ услуг через Интернет;
- 11) поступали ли на мобильное устройство сообщения, содержащие ссылки на интернет-ресурсы, когда, от кого, содержание сообщений, осуществлялся ли переход по данным ссылкам, если да, то каков результат (было установлено приложение, установка приложения неожиданно прервалась, мобильное устройство «зависло», потребовалась перезагрузка, приложение «попросило» ввести определенные данные и пр.);
- 12) ремонтировалось ли устройство до или после обнаружения факта хищения, где, кем;
- 13) поступали ли сообщения о снятии денежных средств, их содержание, номер, с которого они были отправлены;
- 14) местонахождение мобильного телефона в настоящее время;
- 15) желает ли заявитель добровольно предоставить устройство для производства компьютерной экспертизы с указанием необходимых паролей;
- 16) обращался ли заявитель в банк, имеются ли у него выписки о движении денежных средств по карте, ответы по обращениям (в случае наличия таковых, приобщить их к материалам проводимой проверки);
- 17) является ли ущерб значительным для заявителя, если да, то отразить подтверждающие это обстоятельства (состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и

расходов заявителя по состоянию на момент совершения в отношении него преступления).

Особое внимание необходимо обратить на сохранение целостности установленного ПО, операционной системы мобильного устройства после загрузки вредоносного ПО. Вредоносная программа, загруженная на мобильное устройство, содержит в себе важную информацию, утрата которой может негативно отразиться на ходе проверки сообщения и расследования уголовного дела.

С целью получения образа загруженного вредоносного ПО и возврата потерпевшему мобильного устройства в сроки, значительно меньшие сроков производства компьютерной экспертизы, могут привлекаться специалисты соответствующих экспертных подразделений. Исследованием данного образа возможно установить Интернет-ресурсы, которые использовались для администрирования вредоносного ПО, и получить иную информацию, которая может иметь значение для расследования уголовного дела.

Если заявитель производил манипуляции, направленные на форматирование устройства, сброс к заводским настройкам, удаление вредоносного ПО антивирусом, снятие образа ПО и изъятие самого смартфона, то результатов может не быть.

Примерный план семинара

1. Действия сотрудника ОВД при сообщении о совершении дистанционного мошенничества, совершенного посредством телефонного звонка.

2. Алгоритм действий сотрудника ОВД при получении заявления (сообщения) о дистанционном мошенничестве, совершенном с использованием сети Интернет.

3. Особенности проведения мероприятий по факту хищения денежных средств с использованием вредоносного ПО.

Вопросы для самоконтроля по теме

1. Укажите распространенные способы совершения преступлений в сфере ИКТ.

2. Какие вопросы подлежат выяснению у лица, сообщившего о факте дистанционного мошенничества, совершенного посредством телефонного звонка?

3. Какие вопросы подлежат выяснению у лица, сообщившего о факте дистанционного мошенничества, совершенного с использованием сети Интернет?

4. Какие вопросы подлежат выяснению у лица, сообщившего о факте хищения денежных средств с использованием вредоносного ПО?

5. Укажите обстоятельства, подлежащие выяснению на стадии возбуждения уголовного дела.

6. На какие федеральные законы следует ссылаться при подготовке запросов в банки и операторам сотовой связи?

7. Какую информацию и каким способом можно получить в свободном доступе в сети Интернет, зная номер банковской карты? Каким образом можно реализовать полученную информацию для раскрытия преступления?

8. Как в свободном доступе в сети Интернет можно установить принадлежность оператору и региону абонентских номеров, использовавшихся при совершении мошенничества?

9. Какую значимую информацию можно получить в рамках ОРМ на стадии возбуждения уголовного дела?

10. Каких специалистов можно привлечь в рамках проверки заявления о совершенном преступлении в сфере ИКТ? Какую значимую информацию можно от них получить?

Тема 3.2. Особенности возбуждения уголовных дел по преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Источниками сообщений о преступлениях, совершенных с использованием ИКТ, являются как физические, так и юридические лица, чьим интересам противоправными действиями других лиц причинен ущерб. Информация о преступлении может поступить в ОВД любым способом: по телефону дежурной части, лично от лица, пострадавшего от противоправных деяний, по сети Интернет, письменным сообщением, направленным почтовой связью.

Разные способы поступления информации о преступлении определяют временные рамки и условия начала процессуальной деятельности, однако, независимо от используемого формата обращения, отправной точкой является момент регистрации сведений в КУСП (книга учета сообщений, преступлений) и составление «Протокола принятия устного заявления о совершенном преступлении», отражающем информацию о предупреждении лица об уголовной ответственности за заведомо ложный донос по ст. 306 УК РФ.

Поводом к возбуждению уголовного дела о преступлениях, совершаемым с помощью ИКТ, помимо непосредственного обращения граждан, может быть рапорт сотрудника полиции об обнаружении признаков преступления (в случаях, когда информация о преступлении поступает от лица, опосредованно владеющего информацией о преступлении или получения ее в результате ОРМ).

Большинство преступлений, совершаемых с использованием ИКТ, относится к преступлениям с материальным составом, поэтому местом их совершения следует признавать место наступления общественно опасных последствий в виде причинения материального ущерба потерпевшему.

В соответствии с указанием МВД России от 13 июля 2015 г. № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества» при поступлении заявления (сообщения) о совершении мошеннических действий с использованием мобильных средств связи проводят проверку, и при наличии в деянии признаков преступления решение о возбуждении уголовного дела принимает территориальный орган, принявший заявление (сообщение).

Осмотр места происшествия является основополагающим следственным действием. При осмотре следователь (дознатель) наблюдает и фиксирует следы преступления. Полученные в ходе осмотра

места происшествия результаты должны быть проанализированы всеми членами СОГ. На основе этих результатов решается вопрос о возбуждении уголовного дела, разрабатываются версии по делу, намечается согласованный план проведения следственных и оперативно-розыскных действий.

Проверка версий осуществляется как следственным, так и оперативно-розыскным путем. Совместный анализ собранных доказательств позволяет обнаружить дополнительные возможности для их проверки и оценки, а также собирания новых доказательств.

На членов СОГ на стадии доследственной проверки распространяется право, предусмотренное ч. 1 ст. 144 УПК РФ:

- получать объяснения от заявителя и других лиц, владеющих информацией, сотрудников кредитных учреждений и операторов связи, которые могут сообщить сведения об обстоятельствах происшествия;
- истребовать документы, предметы (например, договоры об оказании банковских услуг и услуг связи, информацию по операциям с использованием платежной карты, чеки и журнальные ленты банкоматов, выписки по счетам, сотовые телефоны, платежные карты и т. д.);
- производить осмотр места происшествия (например, места установки платежных терминалов, банкоматов и других), в ходе которого фиксируются следы преступления и решаются задачи по поиску возможных источников доказательств (в частности, устанавливается наличие камер видеонаблюдения);
- осматривать предметы (документы);
- производить освидетельствование лиц на предмет наличия особых примет;
- назначать судебные экспертизы и получать заключение эксперта.

Содержание стадии возбуждения уголовного дела сводится к установлению обстоятельств совершенного преступления, поэтому на данном этапе УПК РФ позволяет производство только четырех следственных действий: осмотр места происшествия, осмотр предметов документов, освидетельствование и назначение судебных экспертиз. Решая вопрос о возбуждении уголовного дела, следователь (дознаватель) оценивает содержание поступивших материалов. Установив где, когда, при каких обстоятельствах, каким способом, кем совершено преступление, его цели и мотивы, он выносит соответствующее постановление (ст. 146–149 УПК РФ).

Примерный план семинара

1. Источники поступления сообщений о преступлениях, совершенных с использованием современных ИКТ.

2. Следственно-оперативные группы, их назначение в раскрытии преступлений в сфере ИКТ.

Вопросы для самоконтроля по теме

1. Что является поводом для возбуждения уголовного дела по преступлениям в сфере ИКТ?

2. На решение какого вопроса нацелено указание МВД России от 13 июля 2015 г. № 1/5562 «Об организации работы по противодействию отдельным видам мошенничества»?

3. Какие виды следственно-оперативных групп существуют?

4. Правовая регламентация, цели и задачи следственно-оперативных групп.

5. Кто осуществляет руководство следственно-оперативной группой?

6. Укажите уголовно-процессуальный инструментарий для проверки информации о преступлении.

7. Укажите следственные действия, которые могут быть выполнены на стадии доследственной проверки.

Тема 3.3. Электронный носитель информации как техническое средство, содержащее значимую для уголовного дела информацию

Компьютерные технологии активно применяются практически во всех сферах деятельности человека, что способствует постоянному развитию и совершенствованию систем, обрабатывающих существенные массивы информации. Для ее получения, копирования, дистанционного обмена, а также для долгосрочного хранения в настоящее время используются различные виды электронных носителей. В Федеральном законе от 28 июля 2012 г. № 143-ФЗ введена новая правовая категория – электронный носитель информации. В соответствии с п. 3.1.9 ГОСТ 2.051-2013, «электронный носитель: материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники».

Необходимость в проведении судебных компьютерных экспертиз электронных носителей информации возникает при расследовании широкого спектра уголовных дел, возбужденных по следующим статьям Уголовного кодекса Российской Федерации: ст. 146 «Нарушение авторских и смежных прав», п. «г» ч. 3 ст. 158 «Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса)», ст. 159 «Мошенничество», ст. 159.3 «Мошенничество с использованием электронных средств платежа», ст. 159.6 «Мошенничество в сфере компьютерной информации», ст. 205.2 «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма», ст. 228.1 «Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», ст. 242 «Незаконные изготовление и оборот порнографических материалов или предметов», ст. 242.1 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютер-

ной информации и информационно-телекоммуникационных сетей», ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования», ч. 2 ст. 280 «Публичные призывы к осуществлению экстремистской деятельности», ст. 280.3 «Публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях», п. «в» ч. 2 ст. 280.4 «Публичные призывы к осуществлению деятельности, направленной против безопасности государства» и др.

Учитывая массовость и многообразие преступлений, совершаемых с применением электронных носителей как технических средств, содержащих криминалистически значимую информацию, их классификация и знания особенностей технического и программного устройства, а также функционирования имеют существенное значение для разработки новых методик судебно-экспертного исследования и последующего корректного их применения сотрудниками экспертно-криминалистических подразделений органов внутренних дел Российской Федерации.

На сегодняшний день имеющиеся в распоряжении экспертно-криминалистических подразделений системы МВД России методики судебно-экспертного исследования позволяют проводить судебную компьютерную экспертизу в отношении следующих объектов, обладающих криминалистически значимой информацией о расследуемом преступлении:

- машинных носителей: накопителей на жестких магнитных дисках; гибких магнитных дисках; CD- и DVD-дисках; flash-накопителей; карт памяти и прочих машинных носителей, информация на которых представлена в виде файловых систем;
- мобильных устройств: сотовых телефонов, смартфонов, планшетных компьютеров и т. п.;
- карт, обеспечивающих доступ к скидкам и льготам (дисконтные, лояльности, бонусные и пр.);

– платежных карт (банковские и небанковские); бывают расчетными (дебетовые), кредитными и предоплаченными;

– специализированных электронных плат, сменных машинных носителей, жестких магнитных дисков автоматов, серверов на системных блоках, интернет-серверов.

Знание видов и основных характеристик электронных носителей информации дает возможность правильно и качественно обнаружить, зафиксировать и изъять электронный носитель, содержащий значимую для расследования уголовного дела информацию, а также при необходимости провести предварительные исследования непосредственно на месте его обнаружения и качественно произвести судебную компьютерную экспертизу в условиях экспертной лаборатории.

Примерный план занятия

1. Понятие электронного носителя информации, их виды.
2. Виды электронных носителей информации.
3. Основные характеристики электронных носителей информации.

Вопросы для самоконтроля по теме

1. Укажите наиболее распространенные виды электронных носителей информации.
2. Назовите способы использования электронных носителей информации.
3. Какие виды электронных носителей информации вы знаете?

Тема 3.4. Производство отдельных следственных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Полнота и объективность расследования преступлений в значительной степени зависит от качества выполнения следственных действий. Последовательность их проведения зависит от следственной ситуации, сложившейся на момент обнаружения признаков преступления. Производство следственных действий осуществляется в соответствии с требованиями, закрепленными ст. 164–170 УПК РФ.

На первоначальном этапе расследования действия следователя (дознавателя) должны быть направлены на установление личности подозреваемого и его местонахождения, выяснение всех обстоятельств совершения преступления. Это позволит выдвинуть всевозможные версии произошедшего события.

Независимо от следственных ситуаций и выдвигаемых версий необходимо установить причины и условия, способствующие совершению преступления, и принять меры, направленные на возмещение причиненного вреда, в том числе путем наложения ареста на имущество.

Рекомендуется ознакомиться с порядком осуществления банковских операций по переводу безналичных денежных средств, находящихся на счетах банковских платежных карт, с использованием средств мобильной связи, а также порядком оказания услуг операторами мобильной связи.

После того, как построены возможные в каждой конкретной ситуации следственные версии, необходимо спланировать ход предварительного расследования.

Планирование расследования включает в себя:

- определение следственных действий, необходимых для установления обстоятельств согласно конкретной следственной версии (допросы, обыски, задержание, осмотры, проведение экспертиз);
- определение содержания и объема следственных действий (какие вопросы целесообразно поставить при допросе каждого участника уголовного судопроизводства, что искать при обыске и где его проводить);
- установление последовательности проведения следственных действий;
- определение времени производства следственных действий;
- выбор мест проведения следственных действий;

- определение документов и предметов, которые необходимо истребовать от кредитных учреждений и операторов связи;
- определение заданий на проведение ОРМ.

Если в процессе совершения мошенничества использовались мобильные средства дистанционной связи, при планировании расследования следует учитывать возможности операторов мобильной связи. Так, оператор сотовой связи имеет возможность идентифицировать с помощью технических средств пользователей сетей связи и определять местонахождение мобильного телефонного аппарата, которым преступники пользовались как на момент подключения к сети, так и в актуальное время. Технические средства операторов мобильной связи и функциональные возможности мобильных телефонных аппаратов обеспечивают постоянное информирование операторов связи в автоматическом режиме о местонахождении мобильного телефонного аппарата. Все сведения об абоненте, его подключениях к сети и местонахождения хранятся операторами связи.

Операторами сотовой связи и ИТКС аккумулируются, обрабатываются и хранятся также сведения в виде текстовой, аудио- и видеоинформации, переданные и полученные абонентами сетей связи, что также учитывается при организации и планировании расследования.

В соответствии со ст. 64 ФЗ «О связи» операторы связи обязаны хранить на территории Российской Федерации:

- информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий;
- текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим ОРД или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

При организации расследования преступлений в целях установления лиц, их совершивших, следователь (дознаватель) может пору-

чить органам, осуществляющим ОРД, получить у операторов связи необходимые сведения о пользователях услуг связи и их действиях в сети.

После установления лица, совершившего преступление, планируются и проводятся следственные действия и ОРМ, направленные на его задержание.

Для изобличения виновного в совершении преступления важное значение имеют не только сведения, полученные от операторов связи, но и фактические данные, полученные при осмотре мобильных телефонных аппаратов и компьютерных устройств, изъятых у подозреваемого.

При осмотре мобильного телефона могут быть получены сведения о содержимом журнала входящих и исходящих соединений, об использовании абонентом интернет-браузеров, скопированы хранящиеся в памяти телефона текстовые сообщения, изображения, видео- и аудиофайлы, а также установлены данные о месте нахождения абонента в конкретный период времени.

При осмотре компьютерного устройства, которым пользовался подозреваемый, можно получить сведения о контактах подозреваемого в социальных сетях, фактах передачи и получения им текстовых и иных сообщений, содержании сообщений и времени их отправления или получения.

Особенности производства отдельных следственных действий. Порядок изъятия электронных носителей информации в ходе проведения следственных действий

Изъятие любых предметов, имеющих значение для уголовного дела возможно в рамках только следственных действий: осмотра места происшествия, обыска или выемки.

Осмотр места происшествия является одним из безотлагательных следственных действий (ч. 2 ст. 176 УПК РФ) и может проводиться как в ходе расследования, так и до возбуждения уголовного дела.

Необходимость его производства по преступлениям, совершенным с использованием ИКТ, как правило, имеется тогда, когда похищенные денежные средства обналичены, например, через банкомат, электронный терминал или др. В этом случае объектом осмотра может признаваться территория (помещение), где расположено техническое средство, предназначенное для совершения операций с использованием платежных карт.

В ходе осмотра следует решать задачи по поиску возможных источников доказательств (в частности, следует установить наличие видеокамер и принять меры по изъятию видеозаписи).

Осмотр места происшествия может быть осуществлен как с участием понятых, так и без них, но с использованием технических средств фиксации следов преступления и вещественных доказательств. Применение фотоаппарата или видеокамеры позволит повысить эффективность осмотра.

По результатам осмотра составляется протокол, в котором указываются: технические средства, используемые при производстве следственного действия; условия и порядок их эксплуатации; объекты, к которым эти средства применены; полученные результаты.

К протоколу осмотра места происшествия прилагаются составленные фототаблицы, схемы. Снимки и иные носители визуальной и звуковой информации, записанные или изготовленные при производстве осмотра места происшествия, являются частью протокола, приложением к нему и так же, как и протокол, имеют статус доказательства.

Составление протокола осмотра места происшествия считается завершенным, когда к нему приобщены снимки и иные носители визуальной и звуковой информации.

Электронные носители информации, изъятые в ходе следственного действия (осмотра места происшествия, обыска, выемки), хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность. После осмотра и производства неотложных следственных действий, если это возможно без ущерба для доказывания, они возвращаются законному владельцу (п. 5 ч. 2 ст. 82 УПК РФ).

В случае невозможности возврата указанных предметов содержащаяся на них информация может копироваться по ходатайству их законного владельца или обладателя содержащейся на них информации (далее – заинтересованные лица). Копирование производится в подразделении органа предварительного расследования на другие электронные носители информации, предоставленные заинтересованными лицами, с их участием и (или) их представителей, а также специалиста в области компьютерных технологий и только в присутствии понятых. При копировании должны обеспечиваться условия, исключающие возможность утраты или изменения информации. Не допускается копирование, если это может воспрепятствовать расследованию преступления. Электронные носители информации, содер-

жащие скопированную информацию, передаются заинтересованным лицам. Об осуществлении копирования информации и о передаче электронных носителей, в соответствии с требованиями ст. 166 УПК РФ, составляется протокол.

Допрос участников уголовного судопроизводства – самый распространенный способ получения доказательств.

При **допросе потерпевшего** – лица, которому непосредственно причинен имущественный вред, – выясняется:

1) когда, где, кем, каким способом и при каких обстоятельствах осуществлен (обнаружен) перевод денежных средств со счета банковской карты;

2) в чем конкретно выражались мошеннические действия и какова их продолжительность (периодичность);

3) дата и время совершения абонентских соединений (отправки SMS);

4) тип и модель использовавшегося мобильного средства связи;

5) какие программы, когда, как и кем установлены на мобильное устройство;

6) какой операционной системой управляется мобильное устройство;

7) как часто используется мобильное устройство и имеет ли оно программы, позволяющие защищать хранящиеся данные;

8) вносились ли изменения в информационную среду (память) мобильного устройства; если да, то кем, и при каких обстоятельствах;

9) характер и размер причиненного вреда;

10) кому известны обстоятельства совершения (обнаружения) преступления или наступившие последствия;

11) кого потерпевший подозревает в совершении преступления и почему.

Следователю (дознавателю) необходимо также выяснить у потерпевшего номер принадлежащего ему банковского счета (банковской карты); пароль доступа к ПО (например, «Мобильному банку»), степень его сложности, а также все детали телефонного разговора с мошенником, отразив в протоколе допроса особенности его речи (темп, речевые дефекты (картавость, шепелявость и др.), употребление специальных слов и терминов – технических, из банковской сферы, а также слов и словосочетаний, носящих ярко выраженный, индивидуальный характер.

В качестве **свидетелей**, как правило, допрашиваются сотрудники банка (кредитной организации), представители оператора мобиль-

ной связи, лица, выявившие преступление, а также иные лица, которым известны обстоятельства совершения преступления или сведения, характеризующие личность подозреваемого.

Общий круг вопросов, подлежащих выяснению при допросе свидетелей, зависит от цели допроса: проверка и уточнение показаний других участников процесса (потерпевшего, подозреваемого, свидетеля, эксперта); получение данных, характеризующих личность участников процесса; получение сведений об особенностях подготовки, совершения, сокрытия преступления, о происхождении обнаруженных и изъятых предметов (документов), их принадлежности, а также об иных обстоятельствах, имеющих значение для уголовного дела.

При допросе свидетелей выясняется:

- 1) как давно они знакомы с потерпевшим и (или) подозреваемым;
- 2) как могут охарактеризовать личность потерпевшего;
- 3) когда, при каких обстоятельствах им стало известно о мошеннических действиях;
- 4) известны ли наступившие последствия и размер причиненного материального ущерба;
- 5) кого подозревают в совершении преступления.

В ходе допроса *сотрудника банка* (кредитной организации) дознавателю необходимо получить информацию о:

- 1) картах (счетах), открытых в банке потерпевшим;
- 2) порядке обслуживания и предоставления дополнительных услуг;
- 3) ПО, предоставляемом держателю банковской карты для удаленного доступа и управления счетом, в том числе, используемом потерпевшим;
- 4) порядке установки и использования ПО;
- 5) требованиях банка, предъявляемых к держателю карты, использующему «Интернет-банкинг» и (или) «Мобильный банкинг»;
- 6) возможности внесения изменений в работу программ третьими лицами;

7) способах получения необходимой информации (какой именно) для совершения операций со счетом банковской карты потерпевшего.

Выясняются также сведения об операторах мобильных средств связи, с которыми заключены договоры о предоставлении удаленного доступа в сеть Интернет по защищенному каналу, способах защиты таких каналов и др.

Из числа представителей мобильного оператора связи рекомендуется допросить в качестве свидетеля системного администратора, который имеет доступ к сетям связи, компьютерной информации и может пояснить об особенностях предоставления соответствующих услуг мобильной связи, включая особенности предоставления удаленного доступа к Интернету по выделенным (защищенным) каналам, для использования соответствующего ПО.

Сотрудники оперативных подразделений, специализирующихся на раскрытии компьютерных преступлений, выявившие преступление и установившие личность подозреваемого также допрашиваются об обстоятельствах, ставших им известными относительно совершенного преступления.

Тактика допроса подозреваемого определяется степенью доказанности вины, сложившейся следственной ситуацией, выбранной линией поведения и выдвигаемыми подозреваемым версиями, отношением к предложению дознавателя дать показания.

В ходе допроса подозреваемого целесообразно выяснить следующее:

- 1) знаком ли он с потерпевшим, если да, то как давно и в каких отношениях с ним состоит;
- 2) когда и по чьей инициативе возник преступный умысел;
- 3) когда, где, кем и каким способом совершены мошеннические действия;
- 4) оказывал ли кто-нибудь помощь, если да, то кто, и в чем она выражалась;
- 5) в чем состояли конкретные действия каждого из соучастников, их данные;
- 6) какая цель преследовалась при совершении мошеннических действий, и по какому принципу проводился отбор потерпевших;
- 7) имеет ли он источник дохода, если да, то каков его размер;
- 8) желает ли он возместить причиненный потерпевшему ущерб.

В ходе допроса подозреваемого необходимо также выяснить уровень его образования, наличие у него профессиональных навыков и иные характеризующие его личность данные.

Имея достаточные основания полагать, что в каком-либо помещении или ином месте находятся орудия преступления, предметы, имеющие значение для уголовного дела, в соответствии со ст. 182 и 183 УПК РФ дознаватель проводит обыск или выемку. Для их производства рекомендуется пригласить специалиста.

Обыск и выемка производятся на основании постановления дознавателя, а обыск в жилище и выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, а также вещей, заложенных или сданных на хранение в ломбард, – на основании судебного решения.

Обыск по уголовным делам рассматриваемой категории производится в целях обнаружения и изъятия средств мобильной связи, компьютерных устройств, носителей компьютерной информации, в том числе вредоносных компьютерных программ, устройств телекоммуникации и иного оборудования, явившихся орудием или средством совершения преступления, а также иных предметов, документов и ценностей, которые могут иметь значение для уголовного дела.

Выемка производится в целях изъятия электронных носителей информации, предметов и документов, имеющих значение для уголовного дела, в случаях, когда точно известно, где и у кого они находятся.

При производстве обыска и выемки могут быть изъяты мобильные телефонные аппараты, электронные записные книжки, пластиковые карты, иные предметы и документы, имеющие значение для уголовного дела.

Упаковать мобильные средства связи, средства компьютерной техники и иные носители компьютерной информации необходимо в специальную упаковку, в которой данную технику поставляет предприятие-изготовитель, либо в картонные и деревянные коробки подходящего размера, уплотнить их прокладками из упругого материала (гофрированного картона, пенопласта, мятой бумаги и др.) с целью исключения перемещения техники внутри упаковки или в полиэтиленовые пакеты подходящего размера.

При выемке документов, как правило, изымаются: договоры о банковском обслуживании и договоры об оказании услуг связи; документы по операциям с использованием платежной карты; банковские чеки и журнальные ленты банкоматов; выписки по банковским счетам потерпевшего и подозреваемого и др.

Подлежит обязательной выемке документ по операциям с использованием платежной карты. Данный документ составляется банком и является основанием для осуществления расчетов по указанным операциям и (или) служит подтверждением их совершения. Он содержит следующие обязательные реквизиты: идентификатор банкомата, электронного терминала или другого технического устройства, предназначенного для совершения операций с использованием платежных карт; вид операции; дату совершения операции; сумму операции; валюту операции; сумму комиссионного вознаграждения или надпись об его отсутствии; код авторизации; реквизиты платежной карты.

При обыске в помещении, занимаемом подозреваемым, наряду с указанными документами изъятию подлежат также документы, удостоверяющие личность, о наличии соответствующего образования и уровне квалификации подозреваемого, а также дневники, записные книжки и черновые записи, содержащие информацию о его социальных связях и деятельности.

Вид, наименование и содержание каждого изымаемого документа отражаются в протоколе обыска или выемки.

Осмотр предметов, имеющих отношение к расследуемому преступлению, обязателен. По уголовным делам рассматриваемой категории осмотру подлежат мобильные средства связи, изъятые у подозреваемого и потерпевшего, а также банковская карта. Осмотр данных предметов рекомендуется производить до назначения экспертизы с участием специалиста в области компьютерной техники.

Осмотр средств мобильной связи состоит из трех основных этапов (наружный и конструктивный осмотры, информационная среда).

При **наружном осмотре** необходимо принять меры к выявлению и изъятию следов рук, оставшихся на его корпусе, крышке аккумулятора отсека с внутренней стороны, на аккумуляторе, внутренней части аккумуляторного пространства, сим-карте. Обнаружение указанных следов позволит назначить дактилоскопическую экспертизу и установить принадлежность и факт использования подозреваемым мобильного средства связи в случае его отказа от этого.

В протоколе осмотра указываются: марка, модель, тип, форма аппарата, цвет корпуса, размер; наличие объективов тыльной и (или) лицевой фото-, видеокамеры (вспышки), фирменных наименований, логотипа, обозначений; количество и расположение функциональных,

встроенных, сенсорных клавиш (джойстика); разъемов для подключения внешних накопителей информации, зарядного устройства, наушников; наличие отверстий для динамика, микрофона, датчиков расстояния и внешней освещенности.

Отдельно указываются особые приметы наружного строения аппарата: повреждения (сколы, царапины, отсутствие должных элементов); наличие дополнительных атрибутов и технических составляющих – чехла, шнура, гарнитуры, графических вставок, надписей и т. п.

В ходе наружного осмотра аппарата производится детальная фотосъемка внешней, оборотной, боковых панелей мобильного телефона. В случае если осматриваемый телефон раскладного или раздвижного типа, то телефон фотографируется в первоначальном и раскладном или раздвижном состоянии.

При **конструктивном осмотре** осматриваются задняя крышка телефона и (или) аккумуляторная батарея (в определенных моделях аппаратов мобильной связи батарея несъемная и встроена в корпус), флеш-карты, сим-карт(ы).

При осмотре аккумуляторной батареи в протоколе указывается ее идентификационный номер, тип, марка, модель, мощность, иная информация, указанная на корпусе аппарата, а также цвет и материал, из которого она изготовлена; при осмотре флеш-карты (MiniSD) – ее идентификационный номер, объем, цвет и материал корпуса.

Сим-карта, обнаруженная в телефоне, осматривается аналогичным образом. В протоколе осмотра описывается имеющийся на ней логотип и наименование оператора мобильной связи.

В ходе конструктивного осмотра проводится детальная фотосъемка внешней и оборотной стороны батареи, флеш-карты, сим-карты, а также тыльной стороны корпуса мобильного телефона (без задней крышки) так, чтобы на снимке был виден идентификационный номер (IMEI) аппарата.

На третьем этапе осмотра (**информационная среда**) исследуются и фиксируются сведения, содержащиеся в памяти мобильного телефона, флеш-карты, сим-карты. В случае, если в ходе осмотра удалось включить мобильный телефон и получить доступ к сведениям, которые в нем находятся, в протоколе в хронологическом порядке фиксируются все производимые в дальнейшем с аппаратом действия и обнаруженная информация.

В случаях, когда при производстве следственных действий мобильный телефонный аппарат изъят во включенном состоянии, вы-

ключать его до осмотра нецелесообразно (отключение может произойти при извлечении батареи, сим-карты, просмотре IMEI-кода на наклейке, расположенной во внутренней части панели телефона, и т. д.), поскольку при последующем включении может потребоваться ввести код блокировки (ПИН-код), который известен только его последнему пользователю. Отказ данного пользователя в предоставлении информации по разблокировке телефона может исключить возможность незамедлительного исследования его информационного содержимого (электронной записной книжки, входящих и исходящих соединений, СМС, ММС-сообщений, e-mail, голосовой почты, фото-, видеофайлов, диктофонных записей, органайзера и др.). В связи с этим в случаях, когда к моменту осмотра телефонный аппарат включен, рекомендуется производить его конструктивный осмотр только после изучения информационной среды.

В случае отказа владельца мобильного телефона в даче согласия на осмотр его содержимого (информационной среды) такой осмотр производится по судебному решению, а в неотложных случаях, в соответствии с требованиями ч. 5 ст. 165 УПК РФ, – без судебного решения с последующим уведомлением суда и прокурора о произведенном осмотре.

Осмотр информационной среды необходимо начать с указания в протоколе процедуры разблокировки клавиатуры телефона, перечисления графических и текстовых элементов, которые отобразились на его экране после разблокировки. Затем осуществляется проверка идентификационного номера (IMEI) мобильного телефона нажатием комбинации клавиш *#06# (пятнадцатизначный номер должен отобразиться на экране телефона).

В случаях, когда информационная среда телефона не защищена паролем, в протоколе осмотра последовательно указывается информационное содержимое телефона – список контактов, сообщений, наличие изображений, фотографий, видеороликов.

При описании имеющегося в журнале вызова конкретного контакта абонента указывается его вид (входящий, исходящий, не отвеченный), время, длительность, данные абонента, с которым осуществлен контакт, а также его абонентский номер (описание сообщения исключает указание длительности, но включает текстовое (СМС) и (или) графическое содержимое (ММС).

Особое внимание при осмотре уделяется информационному содержимому встроенных и (или) съемных носителей информации: контактов, фото-, видео- и аудиофайлов.

Описание графических изображений, фотографий состоит из следующих элементов: описания изображения, типа, размера, времени создания файла (описание видеороликов включает, помимо указанного, их длительность).

В целях извлечения и анализа информационных данных из средства мобильной связи любого типа и вида в следственной и экспертной практике широко используются специальные устройства («Мобильный криминалист», UFED, XRY и др.), позволяющие войти в операционную систему в обход паролей и логинов либо распознавая их, работать с мобильными устройствами без аккумулятора либо отдельно с сим-картой. В случаях, когда доступ к информационной среде мобильного телефона затруднен, для участия в осмотре необходимо привлечь специалиста, имеющего навыки пользования данными устройствами.

В ходе осмотра информационной среды мобильного телефонного аппарата проводится детальная фотосъемка его экрана. Для фиксации большого объема сведений, содержащихся в информационной среде телефонного аппарата, применяется видеосъемка.

Аудио-, видеозапись переговоров потерпевшего с лицами, совершившими преступление, осматриваются для фиксации содержания переговоров и выяснения достоверности записанной информации. В протоколе осмотра фиксируются время звучания записи, содержание той части, которая имеет значение для уголовного дела, и фразы начала и конца фонограммы.

Осмотр банковской карты проводится по общим правилам осмотра предметов и документов.

Рассмотрим **правила получения информации о соединениях между абонентами и (или) абонентскими устройствами**. Информация о соединениях между абонентами и (или) абонентскими устройствами позволяет установить персональные данные абонентов операторов связи, место, время, количество и последовательность соединений между абонентами и абонентскими устройствами, а при необходимости – и содержание отправленных или полученных абонентами сообщений в текстовой или иной форме (в виде фото-, видеоизображений или аудиозаписей).

Правила получения такой информации определены ст. 186¹ УПК РФ, ст. 64 ФЗ «О связи» и постановлением Правительства Российской Федерации от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность».

В соответствии со ст. 186¹ и ч. 1 ст. 165 УПК РФ дознаватель с согласия прокурора возбуждает перед судом ходатайство о производстве рассматриваемого следственного действия и при необходимости принимает участие в судебном заседании.

В ходатайстве указывается организация, которой поручается техническое осуществление получения информации о соединениях между абонентами и (или) абонентскими устройствами. Резолютивная часть ходатайства формулируется следующим образом: «Прошу разрешить получение сведений о том, какие телефонные номера, абонентские устройства или IP-адреса зарегистрированы на проверяемое лицо, и разрешить получение сведений о соединениях с данных номеров, абонентских устройств, IP-адресов» либо «Прошу разрешить получение сведений о том, с какого телефонного номера (абонентского устройства или IP-адреса) осуществлялось соединение с телефонным номером (абонентским устройством или IP-адресом) потерпевшего, свидетеля; на кого зарегистрирован данный телефонный номер (абонентское устройство или IP-адрес) и сведения о данном лице, его адрес проживания, адрес дислокации оборудования (стационарного телефона или точки доступа в Интернет) либо местонахождение абонентского устройства мобильной связи по базовым станциям (биллинг); какие телефонные номера (абонентские устройства или IP-адреса) осуществляли связь по базовым станциям (биллинг), находящимся в таком-то районе, в такое-то время».

После получения разрешения на получение информации о соединениях между абонентами (абонентскими устройствами) дознаватель направляет копию постановления судьи в организацию, осуществляющую услуги связи.

Информация о соединениях между абонентами (абонентскими устройствами) предоставляется операторами связи в печатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов (абонентских устройств).

Получив массив сведений о телефонных переговорах за определенный период времени в пределах определенных базовых станций, дознаватель должен изучить номера телефонов, продолжительность переговоров с этих телефонов и другую информацию, которая позволит идентифицировать абонента, причастного к совершению преступления.

Осмотр документов, содержащих информацию о соединениях между абонентами (абонентскими устройствами), рекомендуется

проводить с участием специалиста. В протоколе осмотра дознаватель указывает ту часть информации, которая, по его мнению, имеет значение для уголовного дела (дата, время, продолжительность соединений, номера абонентов и др.).

Представленные операторами связи документы с информацией о соединениях между абонентами (абонентскими устройствами) приобщаются к материалам уголовного дела в полном объеме на основании постановления дознавателя как вещественное доказательство и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

При расследовании рассматриваемых преступлений возможно назначение и производство различных видов экспертиз, из которых наиболее востребовано исследование электронных устройств, используемых для хищений денежных средств: сотовых телефонов, планшетные и стационарные компьютеры, ноутбуки, т. е. *компьютерная экспертиза*.

В распоряжение эксперта, помимо средств – носителей искомой информации, целесообразно предоставить сведения о соединениях абонентских устройств, полученные от оператора связи и подтверждающие (косвенно указывающие на) совершение определенных действий с электронного устройства, направленные как на перевод денежных средств на счета третьих лиц, так и на завладение необходимой для этого информацией (отправка соответствующих команд посредством СМС, внедрение программ-шпионов, иного вредоносного ПО и др.).

Объектами исследования компьютерной экспертизы также могут быть СВТ и программные продукты: системное ПО (операционные системы), вспомогательные программы – утилиты, служебная системная информация, прикладное ПО, исходные тексты программ и т. п.

В рамках судебной экспертизы могут проводиться *аппаратно-компьютерное, программно-компьютерное, информационно-компьютерное исследования*.

Целью **программно-компьютерного исследования** является изучение функционального предназначения, характеристик, структурных особенностей, текущего состояния, представленного на исследование ПО компьютерной системы.

Объектами программно-компьютерного исследования являются приложения общего назначения – текстовые и графические редакторы, системы управления базами данных, электронные таблицы, ре-

дакторы презентаций, представленные как на электронных носителях, так и на бумажных, исполняемые модули и пакеты программ в различных состояниях (дистрибутив, адаптированная программа, выполняемая программа).

На разрешение эксперта для программно-компьютерного исследования могут быть поставлены следующие вопросы.

1. Может ли разработанный программный продукт использоваться по назначению (например, соответствующее вредоносное ПО)?

2. Какова общая характеристика представленного ПО, из каких компонентов (программных средств) оно состоит?

3. Какую классификацию имеют конкретные программные средства представленного программного обеспечения?

4. Имеют ли программные средства следы преодоления защиты (оказало ли влияние вредоносное ПО на предустановленные лицензионные программы)?

5. Каково наименование, тип, версия, вид представления (явный, скрытый, удаленный) программного средства?

6. Каков состав соответствующих файлов ПО, каковы их параметры (объемы, даты создания, атрибуты)?

7. Какое общее функциональное назначение имеет программное средство?

8. Каково фактическое состояние программного средства, его работоспособность по реализации отдельных (конкретных) функций?

9. Имеются ли на носителях информации тексты (коды) первоначального состояния программы?

Информационно-компьютерное исследование является ключевым при производстве компьютерной экспертизы, так как позволяет завершить целостное построение доказательственной базы путем окончательного разрешения большинства вопросов, связанных с компьютерной информацией.

Объектами информационно-компьютерного исследования являются файлы, подготовленные с использованием программных средств: с расширениями текстовых форматов (txt, doc), графических форматов (bmp, jpg, tif, cdr), форматов баз, данных (dbf, mdb), электронных таблиц (xls, cal).

При производстве информационно-компьютерного исследования в рамках компьютерно-технической экспертизы можно выделить следующие задачи:

– установление свойств и вида представленной информации в компьютерной системе при ее непосредственном использовании;

- определение фактического состояния информации; установление первоначального состояния информации на носителе данных;
- определение времени, хронологической последовательности воздействия на информацию; определение условий изменения свойств исследуемой информации.

Примерным итогом информационно-компьютерного исследования является ответ на следующие вопросы.

1. Какие свойства, характеристики и параметры (объемы, даты создания; изменения, атрибуты) имеют данные на носителе информации?
2. В каком виде (явном, скрытом, удаленном, архивном) информация имеется на носителе?
3. К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа)?
4. Каким образом организован доступ (свободный, ограниченный) к данным на носителе информации, каковы его характеристики?
5. Каковы пользовательские свойства и предназначение данных на носителе информации?
6. Какие данные для решения определенной функциональной задачи имеются на носителе информации?
7. Какие данные о собственнике (пользователе) компьютерной системы (в том числе логины, пароли, права доступа) содержатся на носителях информации?
8. Какие данные с представленных на экспертизу документов (образцов) и в каком виде (целостном, фрагментарном) находятся на носителе информации?
9. Возможен ли доступ в Интернет с представленных на исследование компьютерных средств? Если да, то каким образом осуществлялся доступ?

Более углубленное информационно-компьютерное исследование имеет своей целью ответы на следующие примерные вопросы.

1. Имеется ли в постоянной памяти, на внешних носителях информации электронного устройства информация о том, что пользователь осуществлял работу на данном устройстве в определенный период (указывается дата и время)? Если да, то требуется указать временные отметки, программы, файлы, периферийное оборудование, с которым работал пользователь в указанный период времени.
2. Имеются ли признаки работы представленного электронного устройства в сети Интернет за конкретный период? Каково содержание установок удаленного доступа и протоколов соединений?

3. Имеется ли в памяти устройства информация о его подключении к Интернету? Какие учетные данные использовались для выхода в Интернет? В каких файлах содержатся сведения об использовавшихся логинах и паролях?

4. Имеются ли в памяти устройства признаки (указывается интересующий перечень конкретных признаков) применения вредоносного ПО, неправомерного доступа к данным?

5. Имеется ли в памяти устройства ПО, позволяющее без уведомления пользователя совершать какие-либо действия, передавать определенную информацию и др.? Если да, то какое это ПО, каковы его возможности, содержание и адресат передачи и др.?

6. Имеется ли в памяти устройства ПО, позволяющее сканировать IP-адреса компьютеров пользователей сети Интернет, имеющих открытые для удаленного доступа из сети Интернет ресурсы? Если да, то какое это ПО (название, версии, место расположения на носителе)? Имеются ли данные, свидетельствующие об использовании этого ПО? Если да, то какие именно?

7. Имеется ли в памяти устройства ПО, позволяющее подобрать пароль (захватить его при вводе)? Если да, то какое это ПО (название, версии, место расположения на носителе)?

8. Имеется ли в памяти устройства ПО, позволяющее пользоваться услугами электронной почты? Если да, то, какое это ПО (название, версии)? Имеются ли в постоянной памяти устройства информация о файлах, содержащих почтовые сообщения? Каков адрес электронного почтового ящика, на который получены входящие сообщения?

На разрешение эксперта целесообразно также поставить ряд вопросов, позволяющих установить наличие в имеющихся электронных устройствах:

а) сохраненных текстов (СМС) переписки между подозреваемым и потерпевшим;

б) истории посещения интернет-сайтов;

в) информации о поиске через установленный на устройстве интернет-браузер (Opera, Google Chrome, Internet Explorer, Safari и пр.) сведений, имеющих отношение, например, к существующим вредоносным программам, позволяющим совершать хищения денежных средств со счетов и банковских карт, к способам распространения таких программ; кроме того, могут быть обнаружены конкретные инструкции, носящие обучающий характер, в которых отражены последовательность и существо действий злоумышленников, заготовки

диалогов, шаблоны СМС, которые необходимо использовать при разговоре с потерпевшим (при СМС-общении) в целях провоцирования его к совершению действий, позволяющих завладеть принадлежащими ему денежными средствами;

г) установленных программ, предназначенных для мгновенной пересылки сообщений (например, ICQ), а также переписки (чатов) в этих программах;

д) программ, позволяющих осуществлять видеосвязь, например Skype (скайп), в файлах истории которых могут содержаться также переданные текстовые сообщения;

е) информации об использовании соответствующих интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки);

ж) информации о регистрации в качестве пользователя в социальных сетях, на интернет-ресурсах (форумах), в том числе внутренних сетевых ресурсах интернет-провайдеров, на которых осуществляется обсуждение (обмен информацией), демонстрация и распространение вредоносного ПО, обсуждаются вопросы его создания и пр.;

з) информации, подтверждающей регистрацию подозреваемого в качестве пользователя в локальной сети, организованной интернет-провайдером, в локальной папке пользователя, в которой также могут содержаться полезные для расследования сведения;

и) сохраненных логинов и паролей (например, утилита операционной системы MacOS 10X «Связка ключей» при условии подтверждения пользователем сохранения пароля содержит информацию о логинах и паролях всех когда-либо посещенных сайтов);

к) текстовых документов, фото-, видеофайлов, прямо или косвенно указывающих на причастность пользователя устройства к информации, сопряженной с рассматриваемыми преступлениями.

Проведение **компьютерной экспертизы средств мобильной связи** (мобильного телефона, смартфона, планшетного компьютера, оборудованного слотом для использования сим-карты (модуль идентификации абонента) позволяет:

– установить номер IMEI телефона (смартфона, планшетного компьютера) в привязке к сим-карте, установленной в данном устройстве;

– определить и скопировать всю содержащуюся в памяти устройства информацию (номера из абонентской книжки, СМС, последние набранные номера, входящие вызовы, фото-, видеофайлы и пр.),

– определить и скопировать информацию из чатов (переписка с помощью мгновенных сообщений как текстовых, так и пересылаемых фото- и видеофайлов, с использованием специально предназначенных для этого программ, самыми распространенными из которых являются WhatsApp (ватсапп) и Viber (вайбер), по содержанию которых можно проследить, при каких обстоятельствах было совершено расследуемое преступление.

Данный и другие виды экспертиз по уголовным делам рассматриваемой категории рекомендуется назначать в государственных экспертных учреждениях системы МВД России и Минюста России, сотрудники которых имеют допуски на проведение таких экспертиз.

Примерный план семинара

1. Основные следственные действия, осуществляемые при расследовании преступлений, совершаемых с использованием ИКТ.
2. Осмотр места происшествия по рассматриваемой категории дел и этапы его проведения.
3. Круг субъектов, подлежащих допросу на начальном этапе расследования, и тактические особенности их допроса.
4. Обстоятельства, подлежащие выяснению в ходе допроса различных категорий участников.
5. Тактика проведения обыска и выемки при расследовании преступлений в сфере компьютерной информации.
6. Получение информации о соединениях между абонентами и (или) абонентскими устройствами.

Вопросы для самоконтроля по теме

1. Какая значимая для органов предварительного расследования информация хранится у операторов сотовой связи? Каков срок ее хранения?
2. Каким способом может быть получена значимая информация у оператора сотовой связи?
4. Какие виды следственных осмотров обычно проводят следователи (дознаватели) по преступлениям, совершаемым с использованием ИКТ?
5. Какова процедура и основные правила копирования информации с электронных носителей?
7. Какие участники уголовного процесса подлежат допросу?

8. Какова процедура осмотра мобильного телефона (компьютера)?
9. Каковы правила получения информации о соединениях между абонентами и (или) абонентскими устройствами?
10. В чем заключается сущность компьютерных экспертиз?

Тема 3.5. Участие специалиста при проведении отдельных оперативно-розыскных мероприятий и следственных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Современный уровень использования информационно-телекоммуникационных технологий при совершении преступлений вызывает адекватную реакцию со стороны правоохранительных органов в деятельности по их раскрытию и расследованию. Эмпирические правила и процессуальный порядок обращения с электронными носителями информации диктуют необходимость использования специальных знаний, т. е. неотъемлемым требованием становится участие в оперативно-розыскных мероприятиях и следственных действиях специалиста, как правило, из числа сотрудников экспертно-криминалистических подразделений органов внутренних дел Российской Федерации, специализирующихся на производстве судебных компьютерных экспертиз, что достаточно часто наблюдается при работе сотрудников полиции при расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий.

В научной литературе широко распространена точка зрения, что все оперативно-розыскные мероприятия, связанные с необходимостью осмотра и последующего изъятия электронных носителей информации, а также их предварительного исследования непосредственно на месте обнаружения, требуют от специалистов особой подготовки: наличия специальных знаний в определенной области информационно-телекоммуникационных технологий и (или) свидетельства на право самостоятельного производства судебной компьютерной экспертизы. Однако, несмотря на наличие в ст. 6 «Оперативно-розыскные мероприятия» Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» разрешения на привлечение для участия в оперативно-розыскных мероприятиях специалистов в формулировке: «Должностные лица органов, осуществляющих оперативно-розыскную деятельность, решают ее задачи посредством личного участия в организации и проведении оперативно-розыскных мероприятий, используя помощь должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе», строгих требований к качеству этих специалистов в законе не имеется. Следовательно, описанный аспект в указан-

ном нормативно-правовом документе нуждается в уточнении и конкретизации. При этом вопросы, связанные с процедурой изъятия электронных носителей информации или информации с них, приведенные в п. 1 ст. 15 «Права органов, осуществляющих оперативно-розыскную деятельность» Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», описаны достаточно детально.

В уголовно-процессуальное законодательство Российской Федерации с 8 января 2019 г. введена ст. 164.1. «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», которая регламентирует процедурные вопросы работы при необходимости обнаружения, фиксации, изъятия электронных носителей информации в ходе проведения следственных действий, однако, так же как и в Федеральном законе от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», не представлены конкретные требования к уровню подготовленности привлекаемых специалистов. Очевидно, что для привлечения специалиста следователю необходимо убедиться в наличии у него профессиональных знаний, подтвержденных документами (наличие диплома о высшем образовании и свидетельства на право самостоятельного производства соответствующего вида экспертиз), в зависимости от объектов, с которым ему придется работать: электротехника, информационные системы и процессы, радиосвязь с информацией, автоматизация программирования и автоматизация управления и др. Если объекты информационно-телекоммуникационных систем различны (информация, программное обеспечение или аппаратура), то необходимым видится привлечение нескольких компетентных специалистов для обеспечения высокого качества изъятия всего объема криминалистически значимой информации.

На этапе подготовки к участию специалиста в оперативно-розыском мероприятии или следственном действии обсуждается необходимость в применении специальной аппаратуры, в качестве которой выделяют:

- 1) специализированный лабораторно-исследовательский переносной компьютер со специальным аппаратным и программным обеспечением для просмотра содержимого жестких дисков, компакт-дисков и других электронных носителей информации, которые окажутся на месте происшествия, если на месте отсутствуют другие работающие компьютеры либо их использование специалистом признано нецелесообразным;

2) соединительные кабели и аппаратные средства (адаптер, блок питания – для прямого подключения к компьютерам и сети);

3) портативный или малогабаритный принтер, подключаемый к компьютеру или ноутбуку (для изготовления бумажных протокола осмотра, списка каталогов и файлов, обнаруженных на осматриваемом носителе информации);

4) загрузочные носители (например, USB флэш-карты) с исследовательским и сервисным программным обеспечением;

5) внешний жесткий диск с необходимым программным обеспечением для запуска с него осматриваемого компьютера в ситуации, когда запуск собственной операционной системы невозможен или нежелателен;

6) аппаратура, в том числе цифровая: фото- и видеокамера, фотовспышка;

7) программное обеспечение общего и специального назначения (на исследовательском компьютере): текстовый редактор для составления компьютерной версии протокола; диагностические программы для сбора информации об устройствах, входящих в состав компьютерной системы, их параметрах и техническом состоянии; программы сбора информации о файловой системе на исследуемых носителях; программы получения информации о программах, находящихся в оперативной памяти компьютера, на месте осмотра (обеспечивающие просмотр буфера памяти компьютера); программы определения настроек аппаратуры и свойств программ; программы просмотра и вывода на печать содержимого файлов разных типов.

Кроме того, участникам следственно-оперативной группы под руководством следователя заранее и с учетом мнения приглашенного специалиста необходимо подготовить достаточное количество необходимого в конкретной оперативно-следственной ситуации упаковочного материала для компьютерной техники, электронных носителей информации и документации, которые могут быть изъяты в процессе осмотра (антистатические пластиковые пакеты, крепкие картонные коробки и упаковочная пена, боксы-контейнеры для компакт-дисков и других носителей), цветные самоклеящиеся ярлыки.

В помещениях с несколькими компьютерами допустим последовательный осмотр, т. е. осмотр осуществляется следователем совместно с приглашенным специалистом-компьютерщиком от одного компьютера к другому. Очередность осмотра устанавливается в зависимости от степени связанности компьютера (наличие кабеля связи; обеспечение условия прямой видимости для оборудования, оснащен-

ного инфракрасным портом передачи информации) или удаленности его расположения от основного (опорного) информационного узла (например, от сервера).

Кроме этого, выделяют правила обращения с компьютерной техникой:

1) все включения и выключения компьютерного оборудования должны осуществляться только специалистами либо под их руководством;

2) не производить разъединения или соединения кабельных линий, прежде чем не будет выяснено их назначение, чтобы не допустить ущерба компьютерной системе или информации;

3) вскрытие корпуса системного блока и демонтаж компьютерного оборудования производить только с участием специалиста;

4) не допускать попадания воды, клеев и мелких частиц на устройства ввода-вывода информации компьютеров;

5) применение магнитных искателей, ультрафиолетовых осветителей, инфракрасных преобразователей и других подобных приборов для осмотра компьютерной техники должно быть согласовано со специалистом, чтобы избежать разрушения электронных носителей информации и интегральных микросхем памяти, а также повреждения криминалистически значимой информации.

Проконсультировавшись со специалистом, предпринимаются шаги к уменьшению неудобств, создаваемых нормальной работе организации на период осмотра. Например, разрешается переключиться на резервную компьютерную систему. В бесконфликтной ситуации, характеризующейся совпадением интересов следователя и лиц, находящихся на объекте, подлежащем осмотру, достаточно попросить персонал приостановить текущую работу с компьютерной техникой, не использовать мобильную связь и перейти в другое помещение, где с ними смогут побеседовать сотрудники оперативных подразделений для установления обстоятельств, имеющих значение для расследуемого дела. Лишь затем проводятся все действия, связанные с обнаружением, фиксацией и изъятием электронных носителей или криминалистически значимой информации с них.

Соблюдение правил, приведенных выше, наряду с привлечением компетентных специалистов для участия в оперативно-розыскных мероприятиях и следственных действиях по преступлениям, совершаемым с использованием информационно-коммуникационных технологий, может значительно укрепить доказательственную базу.

Примерный план занятия

1. Подготовка к проведению следственных действий с участием специалиста, порядок его привлечения, разъяснения прав и обязанностей.

2. Использование специальных познаний и технических средств при проведении следственных действий по преступлениям, совершаемым с использованием ИКТ.

3. Участие специалиста при проведении обыска (выемки) и осмотра предметов и документов.

Вопросы для самоконтроля по теме

1. Регламентация использования знаний сведущих лиц в уголовно-процессуальном законодательстве.

2. Понятие и сущность специальных знаний.

3. Формы и цели использования специальных знаний при проведении следственных действий.

4. Порядок и условия участия специалиста в производстве следственных действий.

5. Обязанности и права специалиста.

6. Принципы взаимодействия специалиста и следователя.

7. Участие специалиста в работе следственно-оперативной группы.

8. Участие специалиста на подготовительной стадии проведения следственного действия.

9. Использование технико-криминалистических средств для фиксации хода следственного действия.

10. Порядок применения технико-криминалистических средств выявления, фиксации и изъятия следов на месте их обнаружения.

11. Оказание помощи следователю на завершающем этапе проведения следственного действия, фиксации его результатов и оценки собранных доказательств.

12. Взаимодействие специалиста и следователя при выявлении причин и условий, способствовавших совершению преступления.

13. Основные задачи, решаемые специалистом в ходе осмотра места происшествия.

14. Требования, предъявляемые к специалисту, участвующему в осмотре места происшествия, его обязанности.

15. Психологические особенности работы специалиста в составе следственно-оперативной группы на месте происшествия.

16. Изъятие и упаковка изымаемых объектов следственного осмотра.
17. Особенности обыска как следственного действия.
18. Задачи, решаемые обыском.
19. Подготовка специалиста к участию в обыске.
20. Виды помощи следователю при производстве обыска.
21. Особенности осмотра изымаемых при обыске предметов и вещей.
22. Применение технико-криминалистических средств в ходе обыска.
23. Взаимодействие специалиста и следователя при производстве выемки.
24. Виды помощи следователю при производстве выемки.
25. Техничко-криминалистическое сопровождение выемки.
26. Понятие и цели предварительного исследования следов и других объектов при проведении следственных действий.
27. Методы предварительного исследования.
28. Порядок оформления результатов проведения предварительного исследования.
29. Использование результатов предварительного исследования материальных следов для выявления признаков лица, совершившего преступление, и обстоятельств расследуемого события.
30. Действия специалиста на статической стадии осмотра.
31. Действия специалиста на динамической стадии осмотра.
32. Оказание помощи следователю в изучении объектов осмотра, выявлении их индивидуализирующих признаков, определении относимости объектов осмотра к расследуемому событию.
33. Действия специалиста на завершающей стадии осмотра.
34. Техника безопасности специалиста на месте происшествия.
35. Консультативная помощь следователю при назначении экспертизы, формулировке вопросов в постановлении.
36. Оказание помощи в подготовке материалов на экспертизу и получении образцов для сравнительного исследования.
37. Заключение эксперта и оценка его результатов следователем.
38. Допрос эксперта.
39. Заключение специалиста.

Тема 3.6. Криминалистическое исследование электронных носителей информации, особенности подготовки и назначения судебных экспертиз по уголовным делам о преступлениях, совершаемых с использованием информационно-коммуникационных технологий

Пандемия Covid-19 показала, как легко могут появиться новые методы онлайн-деятельности при изменении социальных потребностей общества. Проявление изменившейся реальности нашлось на всех уровнях: от введения электронного документооборота в разные области до цифровизации системы госзакупок. 2020 и 2021 гг. стали толчком для непосредственного внедрения информационных технологий практически во все: бизнес, социальные и юридические процессы. Согласно данным Главного управления правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации, число киберпреступлений в России заметно выросло в постпандемийный период. Соответственно, возросла актуальность в изучении характера преступлений, совершенных с использованием информационно-телекоммуникационных технологий, посредством получения криминалистически значимой информации о фактах их совершения путем ее обнаружения, фиксации, изъятия с электронных носителей и последующего анализа сотрудником экспертно-криминалистического подразделения системы МВД России для дачи вывода в заключении.

Криминалистическое исследование электронных носителей информации в системе МВД России осуществляется путем проведения судебных компьютерных экспертиз сотрудниками экспертно-криминалистических подразделений. Производство компьютерной экспертизы подразумевает обеспечение доступа к информации (нередко путем ее восстановления), содержащейся в электронных носителях; выявление действий, произведенных с ними и хранящейся в них информацией.

В научной, учебной и методической литературе компьютерную экспертизу принято подразделять на аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную и компьютерно-сетевую экспертизы. Аппаратно-компьютерная экспертиза производится с целью исследования технической части компьютерных средств, а вопросы, выносимые на разрешение, носят, как правило, диагностический характер.

Сотрудники экспертно-криминалистических подразделений системы МВД России выполняют так называемую компиляцию информационно-компьютерной, программно-компьютерной и компьютерно-сетевой экспертиз.

На сегодняшний день, существует несколько основных типовых методик, используемых при проведении экспертного исследования компьютерных устройств носителей информации.

1. «Типовая методика исследования компьютерной информации»: Г.В. Саенко, О.В. Тушканова (2010).

Экспертная задача: поиск компьютерной информации по заданным критериям.

Вопросы, поставленные перед экспертом:

- имеется ли на представленных на исследование машинных носителях (дать перечень) информация, содержащая следующие ключевые слова: (дать перечень ключевых слов);

- имеется ли на представленных на исследование машинных носителях (дать перечень) информация о (изложить о чем).

2. «Типовая методика исследования информации в мобильных телефонах». О.В. Тушканова, В.М. Щербак, С.Н. Сеницын, С.В. Ермолов (2014).

Экспертная задача: поиск информации в мобильных телефонах по заданным критериям.

Вопросы, поставленные перед экспертом:

- установлено ли на исследуемом объекте мобильное приложение WhatsApp (Viber, Telegram и т. д.);

- возможно ли установить дословное содержание переписки в мобильном приложении WhatsApp (Viber, Telegram и т. д.) исследуемого объекта с контактом;

- идентична ли переписка, содержащаяся в мобильном приложении WhatsApp (Viber, Telegram и т. д.), переписке, указанной в протоколе (содержание, дата и время отправки и получения сообщений, адресаты сообщений);

- можно ли сделать определенный вывод об отправке, получении и прочтении абонентами данных сообщений за указанные даты и время;

- имеются ли признаки фальсификации, модификации указанных сообщений с использованием специальных программ, иных технических средств и способов (изменения содержания, подмена отправителя и (или) получателя, изменение даты и (или) времени, искус-

ственного создания неотправленных и неполученных сообщений под видом отправленных и полученных);

- имеются ли требуемые файлы (фото, видео или др.) в файловой системе представленного на экспертизу мобильного телефона (планшета).

3. «Типовая методика исследования информации, находящейся на магнитной полосе платежных карт»: Г.В. Саенко, О.В. Тушканова (2010).

Экспертная задача: исследование информации, находящейся на магнитной полосе платежных карт платежных систем Visa, MasterCard и МИР.

В результате исследования может быть установлено:

- какая информация имеется на магнитной полосе пластиковой карты, представленной на исследование;

- если такая информация имеется, то каким образом она может быть интерпретирована в соответствии с правилами платежных систем;

- соответствует ли информация, записанная на магнитную полосу пластиковой карты, информации, имеющейся в элементах внешнего оформления данной карты;

- может ли представленная на исследование пластиковая карта быть воспринята в технологии функционирования платежной системы в качестве кредитной или расчетной (при условии использования информации, записанной на магнитную полосу карты) на определенную дату или период времени.

При производстве компьютерных экспертиз также широко используются различные методические рекомендации, одной из таких является «Особенности выявления и расследования правонарушений, связанных с незаконной организацией и проведением азартных игр. Использование специальных знаний», составленная ЭКЦ МВД РФ, ГУ СК РФ, ВНИИ МВД РФ в 2016 г.

Экспертная задача: исследование информации, находящейся на специализированных электронных платах автоматов.

В результате исследования (при условии представления электронных плат) может быть установлено:

- как атрибутируют (именуют) себя программы, имеющиеся на представленных электронных платах;

- каковы настройки и статистика работы устройств, из которых изъяты представленные электронные платы;

– соответствуют ли показания даты и времени, имеющиеся на представленных электронных платах, текущим показаниям даты и времени;

– при назначении компьютерной экспертизы (исследования) иных видов игровых автоматов, кроме указанных выше, возможно поставить на разрешение следующие вопросы:

– имеется ли на представленном объекте программное обеспечение, атрибутирующее себя (указать наименование) – при отсутствии образцов для сравнительного исследования;

– имеется ли на представленном объекте программное обеспечение (указать наименование) – при наличии образцов для сравнительного исследования;

– имеются ли сведения о работе программного обеспечения (указать наименование);

– возможно ли с помощью программного обеспечения указать наименование совершить конкретные действия (указание на организацию азартной игры, проведение лотереи и другое недопустимо);

– имеются ли на представленном объекте интересующие следствие сведения (например, о сетевых соединениях, работе в сети интернет, переписке пользователей, учете денежных средств и т. д.);

Эксперты не могут отвечать на правовые вопросы, не должны выходить за пределы своей компетенции. Поэтому недопустимо ставить перед экспертами вопросы, касающиеся, например, отнесения изъятого оборудования к игровому, лотерейному, торговому, развлекательному.

Судебная компьютерная экспертиза дает возможность собрать достаточное количество доказательственной информации, необходимой для раскрытия преступлений и расследования уголовных дел. В последнее время назначается все чаще, поскольку уровень преступлений, совершаемых с использованием информационно-коммуникационных технологий, с каждым годом повышается.

Примерный план занятия

1. Основы криминалистического исследования компьютерных устройств. Виды и задачи криминалистического исследования электронных носителей информации.

2. Способы сокрытия следов преступлений в сфере компьютерной информации.

3. IP-адрес и доменная система имен в следовой картине компьютерных преступлений. MAC-адрес как уникальный идентификатор оборудования компьютерных сетей.

4. Меры предосторожности и обеспечения сохранности информации на электронных носителях.

Вопросы для самоконтроля по теме

1. Что такое компьютерная экспертиза.
2. Какие виды компьютерных экспертиз вы знаете?
3. Какие вопросы ставятся при назначении компьютерных экспертиз?

Перечень нормативных правовых актов, основной и дополнительной учебной литературы

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993.
2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001 № 177-ФЗ.
3. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ.
4. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31.05.2001 № 73-ФЗ в действующей редакции.

Основная литература

1. Методы и способы получения доказательственной информации с электронных носителей: курс лекций / сост. А.В. Скачко. Краснодар: Краснодар. ун-т МВД России, 2014.
2. Баркалова Ю.М. Подготовка экспертов по производству компьютерных судебных экспертиз: метод. рекомендации. Воронеж: Воронеж. ин-т МВД России, 2013.
3. Криминалистика: учеб. / ред. А.Г. Филиппов. 3-е изд., перераб. и доп. М.: Юрайт, 2013.
4. Криминалистика. Углубленный курс: учеб. / ред. А.Г. Филиппов. М.: ДГСК МВД России, 2012.
5. Справочник следователя. Осмотр места происшествия / сост. А.В. Боловинов и др. М.: ЦОКР МВД России, 2010.
6. Скогорева Т.Ф. и др. Организация взаимодействия при раскрытии и расследовании преступлений специализированными подразделениями дознания органов внутренних дел: учеб. пособие. Волгоград: ВА МВД России, 2016.
7. Фадеев И.А. Правовые основы организации взаимодействия следователя и оперативного сотрудника полиции // Рос. следователь. 2014. № 4. С. 10–13.

Дополнительная литература

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика. 3-е изд., перераб. и доп. М., 2008.

2. Введенская О.Ю. Информационно-телекоммуникационная сеть Интернет как источник следовой информации о криминальном событии: фондовая лекция. Краснодар, КрУ МВД России, 2016.

3. Еремченко В.И., Зиновьева Н.С., Алексеенко И.Л. Юридические и организационные аспекты использования информационно-телекоммуникационных систем в целях противодействия экстремистской деятельности в современных условиях: науч.-практ. пособие. Краснодар: Краснод. ун-т МВД России, 2015.

4. Першин А.Н. Криминалистические основы анализа документированной информации в уголовном судопроизводстве. Омск: Омская академия МВД России, 2015.

5. Стельмах В.Ю. Получение информации о соединениях между абонентами и(или) абонентскими устройствами как следственное действие. Екатеринбург: Урал. юрид. ин-т МВД России, 2014.

6. Судебные экспертизы в гражданском судопроизводстве: организация и практика: науч.-практ. пособие / ред. Е.Р. Россинская. М.: Юрайт, 2011.

7. Тактика следственных действий, направленных на отыскание, обнаружение и исследование электронных носителей и информации на них: учеб. пособие / ред.: А.А. Кузнецов, Д.В. Муленков. Омск: Омская академия МВД России, 2015.

4. ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ОБЩЕУГОЛОВНЫМ, ЭКОНОМИЧЕСКИМ И ПРЕСТУПЛЕНИЯМ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Тема 4.1. Выявление и раскрытие преступлений общеуголовной направленности, совершаемых с использованием информационно-коммуникационных технологий

Развитие ИКТ существенно упростило и ускорило действия и процессы, связанные с осуществлением денежных расчетов, что послужило предпосылкой появления новых форм совершения преступлений общеуголовной направленности. К общеуголовным преступлениям, совершаемым с использованием ИКТ, относятся кража (ст. 158 УК РФ) и мошенничество (ст. 159 УК РФ).

Значительная часть мошенничеств с использованием ИКТ, специальных приемов и методов совершения преступлений и сокрытия их следов, противодействием правоохранительным органам совершается преступными группами, в том числе имеющими межрегиональный и межгосударственный характер.

Изучение массива данных о мошенничествах, совершенных с использованием ИКТ, позволяет их структурировать следующим образом.

1. Преступления, связанные с фиктивной продажей товаров или услуг посредством сети Интернет

Преступником создается объявление о продаже товара или оказании услуг на специализированном сайте в сети Интернет¹ (в том числе посредством приложения для мобильных устройств), на форуме в социальной сети², в газете³ или бегущей строкой на телевизионном канале. При публикации объявления указываются реквизиты для обратной связи. Цена товара или услуги, указанная в объявлении, как правило, ниже рыночной, для привлечения внимания потенциального

¹ Например, на сайтах: www.avito.ru, youla.io, drom.ru, kupiprodai.ru, market.yandex.ru и др.

² Например, социальные сети «ВКонтакте», «Одноклассники», «Мой Мир» и др.

³ Например, «Из рук в руки».

потерпевшего. После того, как потерпевший свяжется с преступником, ему предлагается осуществить полную или частичную оплату товара или услуги.

2. Преступления, связанные с фиктивной покупкой товаров или услуг посредством сети Интернет

Преступник анализирует объявления о продаже товаров или предоставлении услуг в Интернете, чаще всего – на специализированных сайтах. Выбрав объявление, преступник звонит потерпевшему и сообщает о своем желании приобрести товар или услугу, для чего он просит сообщить полные данные банковской карты потерпевшего. После этого преступник посредством ресурсов, доступных в сети Интернет¹, предпринимает попытки перевода денежных средств с банковской карты потерпевшего, в некоторых случаях просит сообщить приходящие потерпевшему пароли². После того как потерпевший сообщит необходимые данные, преступник производит перевод денежных средств потерпевшего со счета его банковской карты или карт.

Распространена также форма хищения, связанная с подключением преступника к услугам интернет-банкинга. Преступник просит подойти к банкомату и выполнить действия, якобы связанные с осуществлением платежа. Потерпевший фактически самостоятельно подключает свою банковскую карту к абонентскому номеру преступника и предоставляет ему код для первоначального входа в интернет-банкинг³.

¹ Самые распространенные ресурсы (сервисы) предоставляются кредитными организациями. Общее название таких ресурсов card-to-card (от англ. – с карты на карту). Для перевода необходимо, как правило, введение кода подтверждения операции, которые приходит потерпевшему на телефон.

² В случае, если ресурс, используемый преступниками, не поддерживает технологии 3DSecure или MasterCard SecureCode (принятыми основными платежными системами, такими как Visa, MasterCard, Мир и другими), то СМС-сообщение с кодом потерпевшему не приходит. Ресурсы, не поддерживающие данные технологии, чаще всего связаны с внесением денежных средств на счета сайтов, специализирующихся на азартных играх, ставках на спортивные события и др. Также в отдельных случаях возможна оплата без кода подтверждения услуг телефонной связи некоторых операторов связи, внесение денежных средств на игровые порталы и т.д.

³ В соответствии с п. 2 постановления Пленума Верховного суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного в зависимости от способа хищения образуют состав кражи или грабежа. В связи с этим преступления, совершенные описанным способом, стали квалифицироваться с 2018 г. как кража. Несмотря на изменения, связанные с квалификацией таких преступлений, методики действий по их раскрытию не претерпели существенных изменений и аналогичны применяемым по отношению к иным мошенничествам, совершенным с использованием ИКТ. В связи с этим мы рассмотрим вопросы оперативно-розыскного противодействия преступлениям данной категории вместе с мошенничествами, совершенными с использованием ИКТ.

3. Преступления, связанные с рассылкой СМС-сообщений

Потерпевшим рассылаются СМС-сообщения следующего содержания: «Ваша банковская карта заблокирована ЦБ РФ. Тел. для справок...», «Вы получили приз, дополнительная информация по телефону...», «С Вашей банковской карты списано **** рублей по решению суда. Доп. информация по телефону...», «Банком проводятся операции по защите от краж с банковских карт. Вам необходимо пройти до банкомата и связаться со специалистом банка по телефону...» и т. д.

Если потерпевший звонит, ему предлагается сообщить полные данные по банковской карте, а также приходящие коды подтверждения операций, после получения которых преступником осуществляется списание денежных средств.

Отдельным способом совершения таких преступлений является убеждение преступником потерпевшего пройти к банкомату и выполнить действия, указанные «сотрудником банка». В ходе выполнения данных действий потерпевший подключает услугу «Мобильный банк» к абонентскому номеру, указанному преступником, в отдельных случаях сообщает преступнику логин и пароль для первичного входа и подключения услуги интернет-банкинга. После этого преступник похищает все денежные средства со счетов потерпевшего.

Несколько иначе реализуется алгоритм преступных действий при СМС-сообщениях о выигрыше товара в рекламной акции. Потерпевшему предлагается оплатить налог или пошлину за выигрыш или за его доставку. Преступники нередко создают на несколько дней интернет-сайт с информацией о проведении указанной в СМС-сообщении акции. Сайт может дублировать дизайн известных торговых организаций. Телефоны «победителей», как правило, под предлогом защиты персональных данных приводятся не полностью, а в формате: 890251*****, 890866***** и т. д., т. е. указывается диапазон номеров, на которые преступниками направлялись СМС-сообщения с ложным сообщением о выигрыше. Денежные средства могут направляться любым способом, но чаще переводом на указанный преступником номер банковской карты.

4. Преступления, связанные со звонками на стационарные или мобильные телефоны потерпевших с ложным сообщением о том, что их родственник попал в беду (сбил на машине пешехода, был задержан сотрудниками полиции с наркотиками, избил хулигана, а тот обратился в полицию и др.) и требуются денежные

средства для решения вопроса с правоохранительными органами или выплаты компенсации «потерпевшим»

Преступник звонит потерпевшему и сообщает о факте совершения родственником потерпевшего какого-либо преступления. Как правило, потерпевшими по данному преступлению являются лица пожилого возраста (55–85 лет), женщины (94%), одинокие (87%). Если потерпевший указывает на то, что голос не похож на голос родственника, это объясняется полученными в результате ДТП повреждениям, волнением и т. д., а телефон быстро передается для разговора сообщнику (например, «следователю»), который сообщает, что для компенсации ущерба требуются деньги. Если потерпевший согласен предоставить денежные средства, то «родственник» или «следователь» сообщают, что за ними подъедет третье лицо (83% случаев). Как правило, денежные средства передаются посреднику по месту жительства потерпевшего в квартире, на лестничной площадке или возле дома. Чаще всего посредники подбираются из числа лиц, работающих водителями в фирмах такси (76%), либо лиц, разместивших в сети Интернет объявления о поиске работы, в основном курьерской (24%). В качестве оплаты за услуги посредник берет часть денежных средств, переданных потерпевшим. Реже (17% случаев) потерпевшему предлагается отправить денежные средства самостоятельно.

5. Преступления, связанные с фиктивным предоставлением кредитов

В социальных сетях в Интернете создается фейковый¹ аккаунт, указывающий на принадлежность его владельца к кредитной организации (например «Ольга Сбербанк» или «Василий банк»), либо страница, имитирующая страницу официальных банков, где потерпевший размещает заявку на получение кредита. В социальных сетях преступником распространяется ссылка на данную страницу. Когда потерпевший обращается к владельцу страницы², тот сообщает, что может обеспечить положительное решение банка о предоставлении кредита за предварительное вознаграждение. После получения денежных средств преступник прекращает переписку с потерпевшим и удаляет аккаунт в социальной сети.

¹ От англ. fake – обман, фальсификация.

² Общение может осуществляться как в форме сообщений, доступных для всех посетителей страницы, так и в личных сообщениях. Иногда после первичного обращения потерпевшего, предлагается продолжить дальнейшее общение в одном из мессенджеров.

6. Преступления, связанные с распространением биологически активных добавок (далее – БАД), медицинских аппаратов, «чудодейственных» амулетов, мощей святых, икон

Преступниками в СМИ или посредством обзвона абонентов распространяется информация о проведении бесплатной проверки состояния здоровья. Заинтересовавшемуся потерпевшему предлагается отправить образцы слюны, ногтей, волос по указанному мошенниками почтовому адресу. Адрес, как правило, вымышленный или дублирует адрес известного медицинского учреждения. В ходе беседы преступники стараются выяснить дополнительную информацию о потерпевшем, его возрасте, заболеваниях, артериальном давлении, частоте посещения поликлиник, вероисповедании и т. д. Через несколько дней после отправления потерпевшим образцов¹, ему сообщают о выявленном тяжелом заболевании и предлагают приобрести средство для излечения. Характерной особенностью данного вида мошенничеств является постоянная смена абонентских номеров, используемых преступниками, а также смена исполняемых ролей. Мошенники могут представляться народными целителями, профессорами медицины, экстрасенсами и т. д. Отличительной особенностью мошенничеств данного вида является то, что потерпевшие могут отправлять деньги многократно. Чаще всего денежные средства направляются потерпевшими посредством переводов на предьявителя.

После того, как потерпевшие осознают, что в отношении них было совершено преступление (когда предлагаемые мошенниками БАДы или амулеты и другое не поступают к потерпевшему или когда родственники потерпевших указывают им на факт мошенничества), преступники нередко предпринимают попытки повторного совершения преступления в отношении этих же лиц, меняя используемую легенду. Потерпевшему поступает звонок от имени «следователя прокуратуры» или несуществующего государственного учреждения и сообщается, что лица, которым он отправлял деньги, задержаны, а потерпевшему полагается возмещение ущерба в сумме, многократно превышающей сумму отправлений. Однако для получения компенсации необходимо оплатить, например, «налог» в сумме 13%. После того, как потерпевший направляет нужную сумму, ему сообщается, что расчет суммы компенсации был произведен неправильно и потерпевшему полагается значительно большая сумма. В итоге требуется вновь доплатить разницу в сумме «налога» и т. д.

¹ Факт их получения преступниками не имеет никакого значения.

Для разговоров с потерпевшим используется, как правило, IP-телефония, договор на оказание услуг связи заключается дистанционно под вымышленными регистрационными данными. Преступниками предпринимаются меры по обеспечению анонимизации в сети Интернет. Для совершения преступлений арендуются офисные помещения, привлекаются группы людей, которые проходят специальную подготовку. Полученные денежные средства получают в отделениях банков разных регионов третьими лицами, установление которых затруднительно. Поиск таких посредников преступниками осуществляется посредством сети Интернет, закрытых групп в мессенджерах, а также случайным образом вблизи отделений кредитных организаций. Роль посредников при совершении таких преступлений, как правило, заключается в обналичивании денежных средств, направленных на их имя потерпевшими посредством банковских переводов и последующем направлении данных денежных средств преступникам. Обычно посредники участвуют в совершении мошенничеств данного вида не более одного раза.

Раскрытие преступлений данной категории представляет особую сложность в связи с высокой степенью подготовленности лиц, их совершающих.

При совершении мошенничеств данного вида могут использоваться стационарные и мобильные телефоны и устройства, банковские счета и карты, различные ресурсы сети Интернет, газеты и рекламные печатные издания, телевидение и т. д.

К числу действий оперативных подразделений при проверке заявлений (сообщений) о преступлениях, совершенных с использованием ИКТ, относятся следующие:

- 1) опрос потерпевшего;
- 2) документирование первоначальной информации, полученной от потерпевшего и иных открытых источников информации;
- 3) участие в осмотре места происшествия;
- 4) запрос информации в организациях, оказывавших услуги связи, в том числе у Интернет-провайдеров;
- 5) запрос информации в кредитных организациях, а также иных организациях, оказывающих услуги по переводу безналичных денежных средств и их эквивалентов;
- 6) запрос информации в логистических организациях, фирмах такси и иных организациях и у физических лиц, участвовавших в качестве посредников при совершении мошенничеств с использованием ИКТ;

7) фиксация на материальных носителях первоначальных данных об обстоятельствах преступления;

8) выдвижение версий.

Завершение выполнения перечисленных действий зависит от ряда не всегда зависящих от него факторов, а также может занимать значительный период времени. В частности, на сроки получения вышеуказанной информации влияет, например, региональная специфика, в том числе следственно-судебная практика, наличие специальных каналов связи для получения информации в электронном виде, наличие договорных отношений между ОВД и кредитными организациями, местонахождение кредитной организации или оператора связи и соответствующего ОВД, запрашивающего информацию и множество иных факторов.

Рассмотрим подробнее действия оперуполномоченного при поступлении заявления или сообщения о преступлении, совершенном с использованием ИКТ.

При опросе потерпевшего необходимо установить:

- использованные обеими сторонами абонентские номера мобильной связи;
- адреса электронной почты; доменные имена сайтов;
- сведения об использованных аккаунтах, в том числе в социальных сетях, мессенджерах;
- номера банковских карт, электронных кошельков, а также точное время использования каждого из перечисленных ресурсов.

По каждому из абонентских номеров на первоначальном этапе целесообразно попросить потерпевшего самостоятельно запросить у оператора связи детализацию телефонных соединений. Это возможно как путем личного обращения гражданина в отделение оператора связи, так и посредством приложения для смартфона или личного кабинета абонента на сайте оператора связи, при этом детализация направляется на указанный абонентом адрес электронной почты. В детализации отражается точное время соединений и абонентские номера, использовавшиеся преступниками при совершении преступлений. Данная мера применяется в случаях, когда отсутствует возможность быстрого получения данной информации посредством ресурсов, имеющихся в ОВД.

На официальном интернет сайте Федерального агентства связи (Россвязь) http://www.rossvyaz.ru/activity/num_resurs/registerNum/ или <http://www.kody.su> на вкладке «Коды сотовых операторов» оперативный сотрудник должен самостоятельно определить оператора связи

по абонентским номерам, использованным преступником, установить субъект Российской Федерации, в котором те зарегистрированы. Факт регистрации абонентского номера в субъекте Российской Федерации не означает факт нахождения там преступника. Данную информацию можно также получить посредством приложений для смартфонов, например «Сотовые операторы».

В дальнейшем запрашивается информация у операторов связи:

а) о регистрационных данных абонентских номеров, использованных преступником для совершения мошенничества;

б) о фактах пополнения баланса данных абонентских номеров с указанием даты, времени, сумм, данных банковских карт (банковских счетов, электронных кошельков и др.), посредством которых пополнялся баланс абонентских номеров мошенников;

в) о фактах пополнения баланса других абонентских номеров с использованием абонентских номеров мошенников

г) о соединениях между абонентами и (или) абонентскими устройствами, включая информацию о типе, направлении, продолжительности соединения, базовой станции, посредством которой оно осуществлялось, и ее азимуте.

При необходимости получения указанных сведений сотрудник оперативного подразделения в своих действиях руководствуется ФЗ «О связи» и ФЗ «Об оперативно-розыскной деятельности», включая получение разрешения суда в порядке, предусмотренном ст. 9 ФЗ «Об оперативно-розыскной деятельности». Полученная информация может быть передана следователю в установленном порядке для приобщения к материалам уголовного дела.

При использовании для совершения преступления электронной почты целесообразно попросить потерпевшего предоставить скриншоты переписки, сделанные таким образом, чтобы кроме текста было зафиксировано точное время отправки и получения письма. Данная информация имеет значение при установлении IP-адреса, с которого осуществлялась отправка письма. Каждое новое использование электронной почты при выходе в Интернет с помощью мобильной связи сопровождается предоставлением пользователю нового динамического IP-адреса.

Если для совершения преступления использовались регистрационные аккаунты на страницах сети Интернет, владельцу либо администратору соответствующего интернет-ресурса направляется запрос о предоставлении информации оперуполномоченным либо следователем по находящемуся в его производстве уголовному делу.

Скриншоты переписки потерпевшего с преступником позволяют при направлении запроса сервису электронной почты конкретизировать время отправки почты до необходимого временного отрезка. Фиксация переписки также может иметь доказательственное значение при задержании подозреваемых и изъятии у них в ходе обысков СВТ, использовавшихся при совершении преступления. Содержание переписки, стилистические и иные особенности письменной речи подозреваемого являются характерными признаками, которые могут способствовать установлению личности преступника.

Аналогичным образом необходимо зафиксировать переписку потерпевшего и преступника в случае, если она осуществлялась посредством мессенджеров.

При опросе потерпевшего целесообразно выяснить, не включена ли в его телефоне функция автоматической записи телефонных переговоров. Нередки случаи, когда такая функция включена и потерпевший об этом не знает или не помнит. При наличии записей переговоров на телефоне, необходимо принять скорейшие меры к их фиксации, не допустив уничтожения ранних записей новыми. Целесообразно произвести выемку записи в порядке, установленном уголовно-процессуальным законодательством. При установлении преступника такие записи также могут иметь доказательственное значение и использоваться при проведении фонетической экспертизы.

При совершении ряда мошенничеств, чаще всего связанных со звонками на телефоны потерпевших с ложным сообщением о попадании их родственника в беду, денежные средства передаются посредникам по месту жительства потерпевшего либо по месту отделения ПАО Сбербанк России. В таком случае необходимо принять участие в осмотре места происшествия, установить и тщательно отработать пути вероятного подхода и отхода предполагаемых преступников, к обнаружению их следов и следов используемых ими транспортных средств, принять меры по установлению свидетелей и очевидцев передачи денежных средств. Полученная информация может иметь поисковое значение, а также использоваться для анализа и выявления серийных преступлений.

После получения первичной информации от потерпевшего, ее фиксации, проведения комплекса мероприятий по месту передачи денежных средств от потерпевшего преступнику необходимо обратиться к учетам ОВД с целью установления фактов совершения аналогичных мошенничеств ранее.

В связи с тем, что централизация полной информации о мошенничествах, совершенных с использованием ИКТ, на федеральном уровне не осуществляется, целесообразно обратиться к региональным криминалистическим учетам. В ряде регионов (Краснодарский край, Алтайский край, Иркутская область и др.) информация о мошенничествах, совершенных с использованием ИКТ, по утвержденным формам (с указанием абонентских номеров телефонов, IMEI, номеров банковских карт и расчетных счетов, доменных имен сайтов, аккаунтов в различных Интернет-ресурсах, электронных кошельков) направляется территориальными подразделениями полиции в региональные информационные центры, где вносится в подсистему ИБД-Ф «Дистанционное мошенничество», по которой возможен экспресс-поиск по нужным реквизитам или словам из фабулы преступления.

При выявлении в учетах аналогичных преступлений необходимо изучить материалы возбужденных уголовных дел, материалов проверки сообщений и заявлений о преступлениях, дел оперативного учета, установить, какие следственные и процессуальные действия, ОРМ проводились ранее, их результаты. В зависимости от результатов, с учетом первичной информации, полученной при опросе потерпевшего, осмотре места происшествия, других мероприятиях, необходимо совместно со следователем выдвинуть версии, запланировать следственные и процессуальные действия, ОРМ по новому преступлению.

Реализация такого алгоритма будет препятствовать дублированию проводимых мероприятий, способствовать координированности действий подразделений ОВД в различных районах и регионах.

На первоначальном этапе также необходимо запросить информацию в учреждениях, предприятиях, организациях, задействованных преступниками при совершении преступления. Первоочередной оперативный интерес представляет информация от операторов связи и кредитных организаций.

У оператора связи запрашиваются:

- регистрационные данные аккаунта (дата и время регистрации; IP-адрес регистрации; последние пять IP-адресов, посредством которых осуществлялось использование аккаунта, дата и время использования; данные, указанные при регистрации, в том числе реальные или вымышленные ФИО; хобби, подписи и цитаты, фотографии, анимационные картинки; «друзья» аккаунта на данном интернет-ресурсе);
- MAC-адрес компьютера (стационарного, планшетного или иного), операционная система;

- адрес электронной почты, посредством которой осуществлялось создание аккаунта и иные привязанные к аккаунту адреса электронной почты;

- иная информация, содержание которой может варьироваться в зависимости от конкретного интернет-ресурса, особенностей ПО, обстоятельств преступления, сроков и времени хранения информации на сервере.

В кредитной организации при наличии у потерпевшего информации о реквизитах счета или банковской карты, на которые он перевел деньги, необходимо получить информацию:

- о лице или организации, на которую зарегистрированы данные счет или карта;

- об абонентских номерах, «привязанных» к данным карте или счету, об абонентских номерах, которые пополнялись с данных карты или счета;

- о наличии дубликатов данной карты и об их количестве;

- о дате, времени, месте и суммах проведенных транзакций и операций по обналичиванию денежных средств.

В кредитной организации также запрашиваются видеозаписи с камер видеонаблюдения и информация о транзакциях по банковской карте или счету с указанием номеров и адресов местонахождения банкоматов и платежных терминалов. В связи с тем, что записи с камер видеонаблюдения и информация о транзакциях хранятся в большинстве случаев в территориально и организационно разобщенных подразделениях банка с учетом ситуаций, когда денежные средства обналичиваются не тем банком, которым выдавалась банковская карта, целесообразно направлять в кредитные организации два различных запроса.

Информация о банковских транзакциях подтверждает факт хищения денежных средств, позволяет установить место их обналичивания. Однако этой информации, как правило, недостаточно для полноценного планирования и осуществления мероприятий, направленных на раскрытие преступления. Полученная из кредитной организации информация подлежит сверке с имеющимися учетами с целью выявления фактов использования абонентских номеров, банковских карт и счетов в совершении аналогичных преступлений.

Информацию кредитных организаций и операторов связи можно получить как в порядке, установленном уголовно-процессуальным законодательством, так и в ходе ОРМ, в связи с чем необходимо раз-

граничение действий оперуполномоченного и следователя по ее получению.

Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» предусмотрены различные процедуры получения информации, составляющей банковскую тайну, для органов, осуществляющих ОРД, и органов предварительного следствия.

Справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются кредитной организацией на основании судебного решения должностным лицам органов, уполномоченных осуществлять ОРД, по их запросам, направляемым в суд в порядке, предусмотренном ФЗ «Об ОРД», при наличии сведений о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией органам предварительного следствия по делам, находящимся в их производстве, при наличии согласия руководителя следственного органа, т. е. для органов предварительного следствия отсутствует необходимость обращения в суд. В связи с этим более целесообразно получать информацию, составляющую банковскую тайну, в порядке, установленном уголовно-процессуальным законодательством.

Получение информации о соединениях между абонентами в порядке, установленном ведомственными НПА МВД России, регламентирующими ОРД, предусматривает проведение мероприятий с использованием ресурсов оперативно-технических подразделений без участия в процессе предоставления информации лиц, не являющихся субъектами ОРД. Тем самым исключается вероятность утечки информации о проводимых ОРМ от сотрудников операторов сотовой связи, т. е. обеспечивается конфиденциальность документирования, а также не требуется время на почтовую пересылку сведений между регионами.

Получение информации о соединениях между абонентскими устройствами возможно также в порядке, установленном ст. 186.1, 165 УПК РФ путем направления оператору связи запроса следователя по уголовному делу, находящемуся в его производстве, с приложением постановления суда.

Выбор способа получения данной информации обусловлен конкретными обстоятельствами раскрытия преступления.

Эффективное сочетание ОРМ и следственных действий, качественное межрегиональное и межведомственное взаимодействие позволяет минимизировать время, необходимое для установления преступников и пресечения их преступной деятельности.

К оперативным подразделениям, взаимодействие которых по раскрытию преступлений, совершенных с использованием ИКТ, имеет приоритетное значение, относятся подразделения уголовного розыска, ПСТМ и оперативно-поисковые подразделения (далее – ОПП).

При взаимодействии подразделений уголовного розыска наиболее важен обмен информацией о совершенных преступлениях данной категории, эффективное и рациональное распределение функций по осуществлению ОРМ, в том числе, в различных регионах, на территории которых зарегистрированы преступления, имеющие признаки серийности.

Лицами, специализирующимися на совершении преступлений с использованием ИКТ, предпринимаются активные меры по обеспечению собственной безопасности, сохранению анонимности в сети Интернет, предотвращению идентификации через используемые средства связи и платежные ресурсы. В связи с этим эффективность раскрытия преступлений, совершенных с использованием ИКТ, существенно повышается с использованием сил и средств ПСТМ и ОПП, дополняющих традиционные средства борьбы с преступностью.

Инициатором мероприятий, проводимых ПСТМ и ОПП, является оперативный сотрудник, которому важно знать организационно-тактические формы мероприятий, выполняемых данными подразделениями, для выбора в конкретной оперативно-тактической ситуации тех форм, реализация которых будет максимально способствовать изобличению преступников и формированию доказательственной базы.

Примерный план занятия

1. Выявление и раскрытие преступлений общеуголовной направленности, совершаемым с использованием ИКТ.

2. Виды преступлений общеуголовной направленности, совершаемых с использованием ИКТ.

3. Действия сотрудников органов внутренних дел при раскрытии преступлений и расследовании уголовных дел, совершенных с использованием ИКТ в зависимости от способа хищения.

4. Порядок и источники получения оперативно-значимой информации, способствующей установлению лица, причастного к совершенному преступлению.

Вопросы для самоконтроля по теме

1. Виды мошенничеств, совершаемых с использованием ИКТ.
2. Действия оперативных подразделений при проверке заявлений (сообщений) о преступлениях, совершенных с использованием ИКТ.
3. Источники получения оперативно-значимой информации.
4. Какую информацию можно получить при запросе в кредитных организациях?

Тема 4.2. Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием информационно-коммуникационных технологий

Основные принципы борьбы с экстремизмом:

- признание, соблюдение и защита прав и свобод человека и гражданина, а равно законных интересов организаций;
- законность;
- гласность;
- приоритет обеспечения безопасности Российской Федерации;
- приоритет мер, направленных на предупреждение экстремистской деятельности;
- сотрудничество государства с общественными и религиозными объединениями, иными организациями, гражданами в противодействии экстремистской деятельности;
- неотвратимость наказания за осуществление экстремистской деятельности.

Противодействие экстремистской деятельности осуществляется по следующим основным направлениям:

- принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности;
- выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

В МВД России вопросы противодействия экстремистской деятельности относятся к компетенции Главного управления по противодействию экстремизму.

Действия сотрудника полиции при обнаружении информации косвенно связанной с темой самоубийств

Согласно ППРФ от 26 октября 2012 г. № 1101 утверждены Правила создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен сайтов, указателей страниц сайтов в ИТКС “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в ИТКС “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено». В соответствии с п. 5 Правил основаниями для включения в данный реестр интернет-ресурсов, распространяющих

информацию о способах совершения самоубийства, а также призывов к совершению самоубийства, являются решения Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор).

Сотруднику полиции, выявившему такую информацию необходимо составить информационное письмо в Роспотребнадзор, в котором указываются URL-адреса интернет-страниц. Сотрудники Роспотребнадзора самостоятельно проверяют указанные интернет-страницы, проведут необходимые исследования, при подтверждении информации направят полученные материалы в Роскомнадзор для ограничения доступа к указанным интернет-страницам.



Министерство Внутренних Дел
Российской Федерации

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ПО
КРАСНОДАРСКОМУ КРАЮ

350020, ул. Дзержинского, 1 г. Краснодар,
тел. 259-50-45, факс. 259-39-18

« » 2019 г. № 8 / -
На № от

Руководителю Управления
Федеральной службы по надзору
в сфере защиты прав потребителей
и благополучия человека по
Краснодарскому краю

советнику государственной
гражданской службы Российской
Федерации 2 класса
М.А. Потемкиной

350000 г. Краснодар, ул.
Рашпилевская, 100

«О направлении сведений»

Уважаемая Мария Александровна!

Согласно Постановлению Правительства Российской Федерации от 26.10.2012 года № 1101, утверждены Правила создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен сайтов, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

В соответствии с п. 5 Правил - основаниями для включения в единый реестр данных, распространяемых посредством сети «Интернет», информации о способах совершения самоубийства, а также призывов к совершению самоубийства - являются решения Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор).

В сети «Интернет» в социальной сети «ВКонтакте» выявлены страницы, в которых активно размещаются сообщения косвенно связанные с темой самоубийств:

- <https://vk.com/id89447888>;
- <https://vk.com/public152589831>;

С учетом изложенного, в целях пресечения деструктивного влияния на детей и молодежь, прошу принять меры по проведению экспертной оценки содержания вышеуказанных «Интернет-ресурсов» и ограничению доступа к ним с учетом компетенции Вашего подразделения.

Начальник
полковник полиции

В.В. Иванов

Действия сотрудника полиции в случае обнаружения в ИТКС информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации

Сотруднику полиции, выявившему такую информацию, необходимо составить информационное письмо в прокуратуру, в котором указываются URL-адреса страниц, на которых размещена такая информация.


**Министерство Внутренних Дел
Российской Федерации**
**ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ПО
КРАСНОДАРСКОМУ КРАЮ**
Центр по противодействию экстремизму
ИНН 2310021269
ул. Гаврилова, 9б, г. Краснодар, 350020
тел. 259-50-45, факс. 259-39-18
« » 2017 г. № 8 / -
На № от

Экс. № ____
Старшему помощнику прокурора
Краснодарского края
по надзору за исполнением законов о
федеральной безопасности,
межнациональных отношениях и
противодействии экстремизму

старшему советнику юстиции
А.В. Рюмину

д.39, ул. Советская, г. Краснодар,
350063

Уважаемый Александр Викторович!

Главное управление МВД России по Краснодарскому краю на постоянной основе осуществляет мониторинг сети Интернет на предмет установления физических и юридических лиц, причастных к экстремистской деятельности.

В результате проведенных мероприятий установлено, что в социальной сети «ВКонтакте» создано сообщество «ПОРА ВЫХОДИТЬ» url-адрес https://m.vk.com/club_8869990?from=quick_search, страница которого доступна для публичного ознакомления неопределенному кругу лиц. При осмотре страницы сообщества «ПОРА ВЫХОДИТЬ» url-адрес https://m.vk.com/club8869990?from=quick_search обнаружены призывы к участию в митинге 26 марта 2017 года по адресу: г. Армавир, площадь им. В. Ленина, проведение которого несогласованно решением Администрации муниципального образования г. Армавир № 01-80/1918/12 от 22.03.2017, т.е. осуществляются призывы к участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

Направляю Вам указанные сведения в порядке информирования, взаимодействия и принятия мер прокурорского реагирования в соответствии со статьей 15.3 (Порядок ограничения доступа к информации, распространяемой с нарушением закона) Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Приложение: Скриншоты на 5 листах; решение Администрации муниципального образования г. Армавир № 01-80/1918/12 от 22.03.2017 на 3 листах.

Начальник
полковник полиции

В.В. Иванов

В соответствии с ФЗ от 28 декабря 2012 г. № 272-ФЗ «О мерах воздействия на лиц, причастным к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации», Генеральный прокурор РФ или его заместители обращаются в Роскомнадзор с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

Роскомнадзор на основании обращения:

- направляет операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, на котором размещена распространяемая с нарушением закона информация;
- определяет провайдера хостинга, владельца интернет-сайта или иное лицо, обеспечивающее размещение указанного информационного ресурса.

В течение суток с момента получения уведомления провайдер хостинга (владелец интернет-сайта) обязан уведомить владельца обслуживаемого информационного ресурса о необходимости незамедлительно удалить распространяемую с нарушением закона информацию.

Действия сотрудника полиции в случае обнаружения в ИТКС экстремистских материалов, включенных в Федеральный список Министерства юстиции Российской Федерации

Федеральный список экстремистских материалов составляется Министерством юстиции России на основе судебных решений. В список входят статьи, листовки, брошюры и произведения изобразительного искусства.

Сотруднику полиции, выявившему такую информацию, необходимо подготовить рапорт на имя непосредственного начальника, к которому приложить скриншоты экрана с изображениями выявленной информации, после чего подготовить письмо в Роскомнадзор.

Начальнику ЦПЭ ГУ МВД России
по Краснодарскому краю

полковнику полиции
И.Л. Иванову

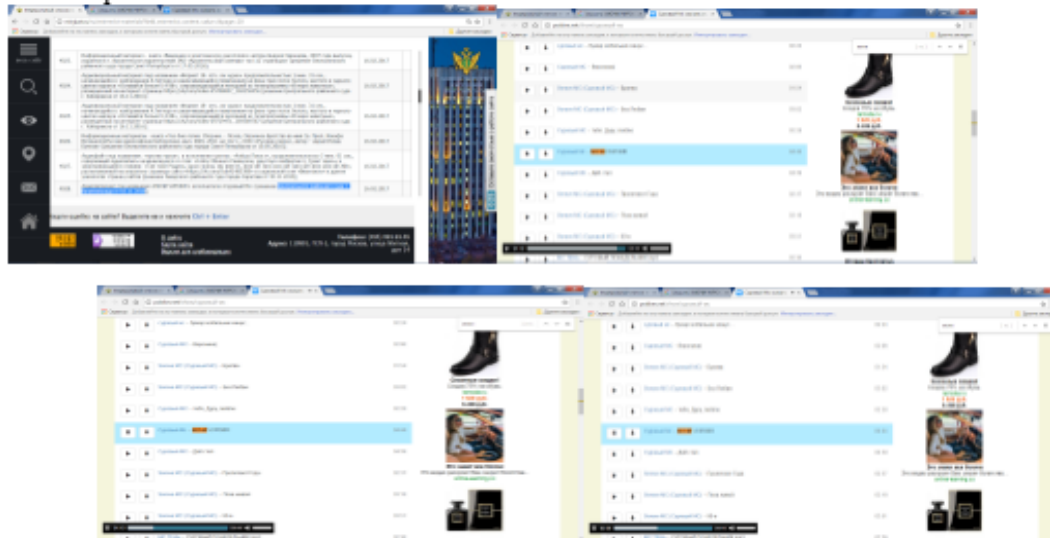
Рапорт

Докладываю, что отделением по информационному противоборству и пресечению содействия экстремистской и террористической деятельности ЦПЭ ГУ МВД России по Краснодарскому краю в рамках реализации Федерального закона «О противодействии экстремистской деятельности» № 114-ФЗ от 25.06.2002 года на постоянной основе осуществляется мониторинг сети Интернет на предмет выявления запрещенных экстремистских материалов.

В результате проведенного мониторинга установлено, что на Интернет странице по ссылке <http://poiskm.net/show/%D1%81%D1%83%D1%80%D0%BE%D0%B2%D1%8B%D0%B9-%D0%BC%D1%81>, в свободном доступе находится Аудиоматериал под названием «МОЧИ ЧУРОК!!!» исполнителя «Суровый Мыс», который внесен в Федеральный список экстремистских материалов под № 4028, на основании Центрального районного суда г. Калининграда от 03.11.2016.

На основании изложенного, прошу Вашего разрешения направить полученные материалы в Управление Роскомнадзора по Южному федеральному округу для ограничения доступа к информации, распространение которой в Российской Федерации запрещено.

Приложение:



Оперуполномоченный ЦПЭ ГУ МВД
России по Краснодарскому краю
майор полиции
«__» марта 20__ года

А.Э. Иванов



МВД РОССИИ
ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО КРАСНОДАРСКОМУ КРАЮ
(ГУ МВД России по Краснодарскому краю)
Центр по противодействию экстремизму
ул. Гаврилова, 96, г. Краснодар, 350020,
«___» _____ 2017 г. № 8/34
на № _____ от _____

Экс. № _____

Руководителю Управления
Роскомнадзора по
Южному федеральному округу

С.Н. Кузенкову

д. 158, ул. Маяковского, г. Краснодар
350001

«О направлении информации»

Уважаемый Сергей Николаевич!

Центром по противодействию экстремизму ГУ МВД России по Краснодарскому краю (далее Центр) на постоянной основе осуществляется мониторинг сети - интернет на предмет выявления запрещенных экстремистских материалов.

В результате проведенного мониторинга установлено, что на Интернет странице по ссылке <http://poiskm.net/show/%D1%81%D1%83%D1%80%D0%BE%D0%B2%D1%8B%D0%B9-%D0%BC%D1%81>, в свободном доступе находится Аудиоматериал под названием «МОЧИ ЧУРОК!!!» исполнителя «Суровый Мыс» которой внесен в Федеральный список экстремистских материалов под № 4028 на основании Центрального районного суда г. Калининграда от 03.11.2016.

На основании изложенного, руководствуясь ст.15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», направляю Вам указанные материалы в целях ограничения доступа информации, распространение которой в Российской Федерации запрещено.

О принятых мерах, прошу Вас проинформировать Центр, с приложением соответствующих решений.

Приложение: на 7 листах.
С уважением

Начальник

И.Л. Иванов

Действия сотрудника полиции в случае обнаружения в ИТКС экстремистских материалов, не включенных в Федеральный список Министерства юстиции Российской Федерации (нацистской атрибутики, символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения)

Пропаганда и публичное демонстрирование нацистской символики или символики, сходной с ней до степени смешения, запрещены в России ст. 20.3 КоАП РФ. В комментариях к Кодексу к нацистской (фашистской) символике относят символику НСДАП, фашистской партии Италии, СС, гестапо. Спорным является отнесение к нацистской символике рейхсвера, вермахта и прочей военной символики

Сотруднику полиции, выявившему такую информацию, необходимо составить рапорт на имя начальника с приложением фотографий экрана с изображенными материалами.

Начальнику ЦПЭ ГУ
МВД России по Краснодарскому краю

полковнику полиции
И.Л. Иванову

Рапорт

Докладываю, что отделением по информационному противоборству и пресечению содействия экстремистской и террористической деятельности ЦПЭ ГУ МВД России по Краснодарскому краю в рамках реализации Федерального закона «О противодействии экстремистской деятельности» № 114-ФЗ от 25.06.2002 года на постоянной основе осуществляется мониторинг сети Интернет на предмет выявления запрещенных экстремистских материалов.

В результате проведенного мониторинга установлено, что на сайте социальной сети «ВКонтакте» создано сообщество «Третий Рейх UA» url-адрес <https://vk.com/public35210286>, страница которого доступна для публичного ознакомления неопределенному кругу лиц. При просмотре страницы сообщества «Третий Рейх UA» url-адрес <https://vk.com/public35210286>, обнаружена демонстрация изображений и фотографий, на которых имелась нацистская атрибутика и символика, а так же атрибутика и символика, сходная с нацистской атрибутикой и символикой до степени смешения, признанная Нюрнбергским международным трибуналом запрещенной.

На основании изложенного, прошу Вашего разрешения направить полученные материалы в прокуратуру Центрального административного округа г. Краснодара для признания информации, распространяемой в сети Интернет, запрещенной к распространению на территории Российской Федерации.

Приложение:



Оперуполномоченный ЦПЭ ГУ МВД
России по Краснодарскому краю
майор полиции

А.И. Иванов

«__» января 20__ года

МВД РОССИИ

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО КРАСНОДАРСКОМУ КРАЮ

(ГУ МВД России по Краснодарскому краю)
Центр по противодействию экстремизму
ул. Гаврилова, 96, г. Краснодар, 350020,
«___» _____ 2017 г. № 8/
на № _____ от _____

Прокурору Центрального
административного округа
г. Краснодара

старшему советнику юстиции
Попову Д.А.

д.36, ул. Седина, Краснодар
350000

«О направлении информации»

Уважаемый Дмитрий Александрович!

Центром по противодействию экстремизму ГУ МВД России по Краснодарскому краю на постоянной основе осуществляется мониторинг сети - интернет на предмет выявления запрещенных экстремистских материалов.

В результате проведенного мониторинга установлено, что на сайте социальной сети «ВКонтакте» создано сообщество «Третий Рейх UA» url-адрес <https://vk.com/public35210286>, страница которого доступна для публичного ознакомления неопределенному кругу лиц. При осмотре страницы сообщества «Третий Рейх UA» url-адрес <https://vk.com/public35210286>, обнаружена демонстрация изображений и фотографий, на которых имелась нацистская атрибутика и символика, а также атрибутика и символика, сходная с нацистской атрибутикой и символикой до степени смешения, признанная Нюрнбергским международным трибуналом запрещенной.

На основании изложенного, направляю Вам указанные материалы в порядке информирования, взаимодействия и принятия мер прокурорского реагирования в порядке ст. 39 Кодекса административного судопроизводства РФ.

О принятых мерах, прошу Вас проинформировать Центр, с приложением соответствующих решений.

Приложение: на 7 листах.

С уважением

Начальник
полковник полиции

И.Л. Иванов

Получив материалы, сотрудник прокуратуры выходит в суд с иском о признании выявленных материалов запрещенными. При удовлетворении судом иска прокурора судебное решение направляется в Управление Роскомнадзора для его исполнения – внесения первичной записи в Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено, и ограничения доступа в отношении такой информации.

Примерный план занятия

1. Виды преступлений террористической и экстремистской направленности, совершаемых с использованием ИКТ.

2. Выявление и документирование преступлений экстремистской и террористической направленности, совершаемых с использованием ИКТ.

3. Мониторинг информационных ресурсов сети Интернет.

4. Методы работы в сетевом информационном пространстве, направленные на противодействие преступлениям экстремистской направленности.

Вопросы для самоконтроля по теме

1. Основные направления противодействия экстремистской деятельности.

2. Алгоритм действий сотрудника полиции в случае обнаружения в информационно-телекоммуникационных сетях информации экстремистского характера, включенных в Федеральный список экстремистских материалов Министерства юстиции РФ.

3. Алгоритм действий сотрудника полиции в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации экстремистского характера не включенных в Федеральный список экстремистских материалов Министерства юстиции РФ.

Тема 4.3. Понятие и сущность криптовалют и других виртуальных активов

Система электронных расчетов – это совокупность определенных правил, технических, организационных, правовых и финансовых процедур, подкрепленных аппаратно-программным комплексом, обеспечивающих возможность осуществлять электронные платежи и переводы в определенной валюте от одного субъекта экономики другому.

Системы электронных расчетов являются особым видом финансово-кредитных систем, позволяющим осуществлять электронные операции без использования наличных денег посредством ИТКС и путем перевода денежных средств по счетам в финансово-кредитных учреждениях и зачетов взаимносформированных требований между экономическими субъектами.

Принципы системы электронных расчетов:

- информативность – анализ потребностей клиентов в электронных расчетах и использовании отдельных информационных технологий;
- целевая ориентация на удовлетворение потребностей клиентов в совершении электронных операций по своим счетам;
- соблюдение указаний, директив контролирующих организаций;
- интеграция всех элементов системы электронных расчетов и обеспечение безопасности совершаемых клиентами операций;
- обеспечение масштабируемости системы электронных расчетов и совместимости внедряемых технологий в существующую систему электронного документооборота.

В ФЗ от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (далее – ФЗ «О НПС») дано определение *электронным денежным средствам* и *электронным средствам платежа*, установлен круг субъектов, которые входят в национальную платежную систему.

Электронные денежные средства – это денежные средства, которые их владелец предоставил другому лицу (оператору) без открытия банковского счета. Например, суды признают, что электронные денежные средства – это доходы, принятые от лиц центром учета переводов интерактивных ставок букмекерских контор (решение Верховного суда РФ от 18 октября 2018 г. № АКПИ18-881). Владелец вправе использовать такие средства для погашения обязательств перед третьими лицами. Владелец средств имеет право передавать распоряжения об операциях с такими деньгами исключительно с исполь-

зованием электронных средств платежа. Закон не отнес к электронным денежным средствам средства, которые получают профессиональные участники рынка ценных бумаг, компании, которые ведут клиринговую деятельность и т. д. (п. 18 ст. 3 ФЗ «О НПС»).

Электронные средства платежа – это технические средства или способы, которые позволяют владельцу электронных денежных средств составлять, удостоверять и передавать распоряжения об операциях с этими средствами (п. 19 ст. ФЗ «О НПС»).

Безналичный денежный оборот, неперсонифицированные платежные продукты, криптовалюта и другие виртуальные активы

В соответствии с ч. 1 ст. 10 ФЗ «О НПС» перевод электронных денежных средств осуществляется:

- с проведением оператором электронных денежных средств полной идентификации клиента физического или юридического лица;
- с проведением упрощенной идентификации клиента – физического лица;
- без проведения идентификации клиента – физического лица.

Использование неперсонифицированных электронных средств платежа (НЭСП) осуществляется клиентом – физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 15 тыс. рублей, а общая сумма переводимых электронных денежных средств с использованием одного НЭСП не может превышать 40 тыс. рублей в течение календарного месяца (ч. 4 и 5 ст. 10 ФЗ «О НПС»).

Криптовалютная сфера заявляется одним из лидирующих направлений развития современных информационных технологий. Многочисленные криптографические проекты не только изменяются формально или функционально, но порой модифицируются в абсолютно новые, необычные форматы. Исходя из этого, применяется следующая классификация криптоактивов:

- 1) базовые криптовалюты;
- 2) альткоины;
- 3) децентрализованные платформы;
- 4) служебные цифровые активы;
- 5) инвестиционные криптографические монеты;
- 6) цифровые товары (криптововары);
- 7) стабильные цифровые монеты (стейблкоины);
- 8) электронные монеты приложений.

Механизм эмиссии и функционирования криптовалют и других виртуальных активов, объем рынка

Криптовалюты частично выполняют функцию платежного средства, поскольку определенные группы экономических агентов готовы принять их в качестве оплаты за товары и услуги. У криптовалют есть ряд отличительных функций, которые выделяют их по сравнению с традиционными платежными средствами:

- отсутствие необходимости в централизованном управлении;
- отсутствие необходимости в большом бюджете для обеспечения безопасности;
- мгновенный вывод средств;
- возможность быстрых международных переводов.

В традиционном понимании эмиссия – это выпуск в свободное обращение новых денег или каких-либо ценных бумаг. Как правило, за эмиссию национальных валют в каждом государстве отвечает специальный орган, который контролирует весь процесс выпуска активов для того, чтобы обеспечить национальной экономической системе некую стабильность и надежность.

Главное отличие эмиссии криптовалют от фиатных денег состоит в том, что при выпуске криптовалют нет единого органа, который занимается контролем выпуска активов.

Майнинг, публичный блокчейн, система распределенного реестра

Централизованные системы хранения и обмена данных имеют ряд недостатков. Среди альтернативных технологий – DLT (Distributed Ledger Technology – технология распределенного реестра). Эта система предусматривает полную децентрализацию: данные хранятся одновременно на всех компьютерах участников сети. Блокчейн – вариант распределенного реестра, децентрализованной сети с равными правами ее участников. Новейшие технологии хранения и обработки информации упрощают взаимодействие пользователей. Ни одна отрасль не осталась в стороне от применения DLT. Финансы, экономика, недвижимость, медицина, образование и другие сферы внедряют технологии распределенного реестра, в том числе блокчейн. Этот вид архитектуры применяется в криптовалютных проектах, где цифровые активы представляют собой особого рода информацию, которая хранится децентрализованно – на компьютерах каждого из участников сети.

Майнинг (от английского *mine* – шахта, *mining* – добыча полезных ископаемых) – деятельность по добавлению новых транзакций (блоков) в блокчейн, за которые оператор транзакции (майнер) полу-

чает вознаграждение в эмитированной криптовалюте. Поэтому майнинг упрощенно считают добычей криптовалюты. Процедура майнинга сводится к серии вычислений по заданному алгоритму с перебором параметров для нахождения криптографического хеша (уникальной битовой строки установленной длины) по массиву заданных входных данных, определяемых хешем предыдущего блока и цепочки блоков в целом. Разные криптовалюты используют разные модели вычислений, но они всегда достаточно длительны по времени и требуют больших вычислительных ресурсов. Успешное завершение вычислений сопровождается добавлением блока в блокчейн по аналогии с внесением транзакции в бухгалтерский реестр. Чем больше блоков вычислено к моменту вычисления текущего блока, тем выше трудоемкость вычислений. Тем самым стоимость каждой новой эмиссии единицы криптовалюты возрастает, что приводит к росту курса криптовалюты в целом. Блоки в блокчейн добавляются и вследствие иных транзакций, например перевода криптовалюты от одного владельца другому. Генерация нового блока операций подтверждается валидаторами – сетевыми узлами проверки. Они сверяют корректность транзакции (при майнинге – вычисления хеша) по специальному алгоритму. Если подставить этот код к старым записям, можно проверить достоверность изменений.

Альтернативными формами приумножения криптовалют в блокчейне являются *форджинг* (аналог начисления процентов на депозит) и *ICO, т. е. краудсейл* (аналог доходов на рынке вторичных ценных бумаг).

В блокчейне можно создать автоматически выполняемое соглашение между двумя и более сторонами – смарт-контракт. Это аналог обычных юридических соглашений, закрепленный в сети с помощью алгоритмов. Условия смарт-контрактов прописываются заранее и выполняются программой. Изменить такой договор в одностороннем порядке невозможно. Программа содержит требования к каждому из участников процесса, контролирует их выполнение. В 2021 г. большинство смарт-контрактов заключалось в блокчейне Ethereum.

Операторы информационных систем, криптобиржи

Цифровые монеты можно хранить в электронных кошельках, обменивать и продавать другим пользователям. Торговля криптовалютой ведется на биржах. Это multifunctional системы, на которых происходит конвертация фиатных денег в цифровые. Токены

(аналог ценных бумаг в цифровой экономике) и коины (цифровые монеты) также можно обменивать между собой. Покупка монет считается вторым способом их получения после майнинга.

Главное преимущество бирж перед финансовыми брокерами – возможность купить активы не только за фиатные средства, но и обменивать одни токены на другие по текущему курсу.

Торговля цифровыми монетами ведется по принципам, которые используются в традиционных финансовых операциях. Однако есть отличия:

1) криптовалюта характеризуется высокой волатильностью (изменчивостью курса);

2) цена на электронную валюту формируется спросом и предложением без дополнительных регуляторов;

3) из-за высокой волатильности инвестиционные портфели из криптовалют не могут быть застрахованы.

Криптовалютные биржи работают без перерывов и выходных, что позволяет приобретать и продавать монеты, не привязываясь к часовому поясу или личному графику. Работа на них ведется по общему алгоритму: регистрация, пополнение счета фиатными деньгами или криптовалютой, оформление заявки на покупку или продажу актива, вывод фиата на банковские счета или электронные системы, отправка цифровых монет на криптовалютные кошельки. Регулирующие компании ограничивают максимальный депозит с учетом действующего законодательства страны, в которой они зарегистрированы. Также существуют лимиты на ввод и передачу активов, хранение их внутри биржи и некоторые другие.

Нормативно-правовое регулирование криптовалют и других виртуальных активов в Российской Федерации

8 апреля 2022 г. Минфин России внес на рассмотрение доработанный законопроект о регулировании цифровых валют. Первый проект ФЗ «О цифровых финансовых активах» появился в 2018 г. и рассматривался до 2020 г. Сейчас это ФЗ от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

В феврале 2022 г. Центральный банк предложил полностью запретить оборот и майнинг криптовалют в России. Основные причины – вывод капитала из страны, уход от налогов, финансирование преступной деятельности и высокие риски для частных инвесторов.

Сейчас законопроект предусматривает комплексное регулирование рынка криптовалюты. Основная задача – сделать транзакции

прозрачными и отслеживаемыми. Чтобы российский пользователь мог законно инвестировать в криптовалюту, ему нужно пройти идентификацию.

В российском законодательстве определение понятия «имущество» не имеет четких границ. В ст. 128 ГК РФ есть понятие «иное имущество», в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права). Список иного имущества не является закрытым, и отсутствие в нем не означает, что объект нельзя отнести к имуществу. Иными словами, можно считать, что криптовалюта является объектом гражданско-правовых отношений. Это подтверждают судебные процессы, которые затрагивали оборот криптовалют. В 2019 г. в ГК РФ появилась новая ст. 141.1 «Цифровые права», в которой определено, что можно считать цифровым активом и кто является его владельцем.

Цифровые права, имущественные права

Под цифровыми правами, согласно ст. 141.1 ГК РФ, понимаются «названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам».

Из определения цифровых прав следует, что норма носит декларативный характер. Конкретные виды цифровых прав должны быть установлены отдельным законом. Можно предположить, что впоследствии отдельным законом к цифровым правам будут отнесены токены и криптовалюты.

Обязательным признаком цифровых прав является то, что их осуществление и распоряжение ими возможны только в информационной системе и не требуют обращения к какому-либо третьему лицу. Под понятие цифровых прав попадают только те объекты, по которым какое-либо лицо несет обязательства. Следовательно, к цифровым правам могут относиться токены и криптовалюты, выпускаемые конкретными компаниями, но при этом классические криптовалюты (Bitcoin и т. п.) к цифровым правам относиться не могут.

Российская ассоциация криптовалют и блокчейна (РАКИБ) – официальное объединение сторонников криптовалют, блокчейна и продуктов на этой базе. Ассоциация представляет интересы криптосообщества в Российской Федерации. В ее деятельности выделяют три направления: криптовалюты, блокчейн и ICO.

Своей целью РАКИБ называет продвижение блокчейн-технологий в стране, формирование предпринимательства в этой области, создание удобного правового фона для всех участников.

Уставные цели РАКИБ:

- максимально широкое продвижение и пропаганда технологии блокчейн, искусственного интеллекта и продуктов, созданных на их основе в интересах развития цифровой экономики;
- защита на российском и международном рынках, в государственных, судебных и правоохранительных органах законных профессиональных интересов, членов ассоциации, внедряющих у себя технологии, направленные на цифровизацию производственных процессов с использованием технологии блокчейн, искусственного интеллекта и продуктов, созданных на их основе;
- создание и внедрение отраслевых технологических и бизнес-стандартов для участников Ассоциации, обеспечивающих их успешное развитие.

Международный опыт нормативно-правового регулирования криптовалют и других виртуальных активов

В настоящее время не существует единого стандарта в регулировании оборота криптовалют. Зарубежные регуляторы руководствуются своим подходом: от разрешения и «традиционного» регулирования в сфере платежей до полного и категорического запрета на данный вид деятельности.

Например, в 2013 г. министерством финансов Федеративной Республики Германии было вынесено постановление о признании биткоина в качестве официального средства расчетов. Требуется только получение лицензии для использования биткоина в коммерческих целях. Германские компании, использующие биткоин, контролируются Федеральным управлением по финансовому надзору. От таких компаний требуется регулярная отчетность, наличие детального бизнес-плана и квалифицированных сотрудников, минимальный размер уставного капитала не менее 750 тыс. евро и использование методов противодействия финансированию терроризма и легализации доходов, полученных преступным путем.

После банкротства биржи криптовалюты Mt.Gox правительство Японии заявило о важности налогообложения и регулировании криптовалюты, в частности биткоина. Тем не менее дальше заявления дело не пошло, никаких конкретных шагов предпринято не было.

Из-за федеративной формы устройства США регулирование криптовалюты – прерогатива отдельных штатов. В штате Нью-Йорк в 2021 г. обсуждалась необходимость введения специальных лицензий для криптовалют, чтобы обязать биткоин-стартапы вести дополни-

тельные документы по операциям. Штат Вашингтон стал первым, объявившим цифровую валюту деньгами. Штат требует от компаний, желающих пересылать цифровые деньги резидентам данного штата, проверять наличие лицензии UMMA.

Революционный скачок в сфере криптовалюты произвела Беларусь. 21 декабря 2017 г. президент Республики Беларусь Александр Лукашенко подписал декрет № 8 «О развитии цифровой экономики». Благодаря этому документу Беларусь стала первой в мире страной со всеобъемлющим правовым регулированием криптовалютных операций и деятельности физических и юридических лиц, связанной с технологией блокчейн.

Примерный план занятия

1. Понятийный аппарат электронных финансовых расчетов. Электронные средства платежа, электронные денежные средства. Безналичный денежный оборот, неперсонифицированные платежные продукты, криптовалюта и другие виртуальные активы.

2. Механизм эмиссии и функционирования криптовалют и других виртуальных активов, объем рынка. Майнинг, публичный блокчейн, мультиподпись, система распределенного реестра. Операторы информационных систем, криптобиржи.

3. Нормативно-правовое регулирование криптовалют и других виртуальных активов в Российской Федерации. Цифровые права, имущественные права. Российская ассоциация криптовалют и блокчейна.

4. Международный опыт нормативно-правового регулирования криптовалют и других виртуальных активов.

Вопросы для самоконтроля по теме

1. Дайте определение системы электронных расчетов. Каковы основные принципы ее функционирования?

2. Чем отличаются электронные денежные средства от электронных средств платежа?

3. В чем состоит привлекательность криптовалюты как финансового актива и платежного средства?

4. Что такое блокчейн?

5. Как производится эмиссия и покупка криптовалют?

6. Как работает криптовалютная биржа?

7. Как нормативно регулируются операции с криптовалютой в Российской Федерации?

Перечень нормативных правовых актов, основной и дополнительной учебной литературы

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993. Доступ из справ. правовой системы «Гарант».
2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001 № 177-ФЗ. Там же.
3. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. Там же.
4. Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ. Там же.
5. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31.05.2001 № 73-ФЗ. Там же.
6. О национальной платежной системе: федер. закон от 27.06.2011 № 161-ФЗ. Там же.
7. О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1. Там же
8. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31.07.2020 № 259-ФЗ. Там же.
9. Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение Центрального банка Российской Федерации от 24.12.2004 № 266-П. Там же.
10. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного суда Российской Федерации от 27.12.2007 № 51. Там же.
11. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48. Там же.

Основная литература

1. Методы и способы получения доказательственной информации с электронных носителей: курс лекций / сост. А.В. Скачко. Краснодар: Краснодар. ун-т МВД России, 2014. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
2. Баркалова Ю.М Подготовка экспертов по производству компьютерных судебных экспертиз: метод. рекомендации. Воронеж: Во-

ронезский институт МВД России, 2013. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

3. Криминалистика: учеб. / ред. А.Г. Филиппов. 3-е изд., перераб. и доп. М.: Юрайт, 2013.

4. Криминалистика. Углубленный курс: учеб. / ред. А.Г. Филиппов. М.: ДГСК МВД России, 2012.

5. Справочник следователя. Осмотр места происшествия / сост. А.В. Боловинов и др. М.: ЦОКР МВД России, 2010.

Дополнительная литература

1. Введенская О.Ю. Информационно-телекоммуникационная сеть Интернет как источник следовой информации о криминальном событии: фондовая лекция. Краснодар, КрУ МВД России, 2016. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

2. Еремченко В.И., Зиновьева Н.С., Алексеенко И.Л. Юридические и организационные аспекты использования информационно-телекоммуникационных систем в целях противодействия экстремистской деятельности в современных условиях: науч.-практ. пособие. Краснодар: Краснодар. ун-т МВД России, 2015.

3. Першин А.Н. Криминалистические основы анализа документированной информации в уголовном судопроизводстве. Омск: Омская академия МВД России, 2015. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

4. Стельмах В.Ю. Получение информации о соединениях между абонентами и(или) абонентскими устройствами как следственное действие. Екатеринбург: Уральский юридический институт МВД России, 2014. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

5. Судебные экспертизы в гражданском судопроизводстве: организация и практика: науч.-практ. пособие / ред. Е. Р. Россинская. М.: Юрайт, 2011.

6. Тактика следственных действий, направленных на отыскание, обнаружение и исследование электронных носителей и информации на них: учеб. пособие / ред.: А.А. Кузнецов, Д.В. Муленков. Омск: Омская академия МВД России, 2015.

7. Волкова Г.П., Махова И.В., Чистова Л.Е. и др. Расследование отдельных видов мошенничества: учеб. пособие. М.: Юрлитинформ, 2014.

8. Голдовский И.М., Гончарова М.Ю., Грачев А.Н. и др. Бизнес-энциклопедия «Платежные карты». М.: Кнорус, 2014.

9. Лебедев В.М. Комментарий к Уголовному кодексу Российской Федерации. М., 2014. С. 896

10. Лебедева А.А. Расследование хищений, совершенных с использованием поддельных банковских платежных карт // Библиотека криминалиста. 2013. № 3.

11. Филиппов М.Н. Особенности расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов. М.: Юрлитинформ, 2014. С. 58.

5. ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ ПО ЛИНИИ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Тема 5.1. Противодействие незаконному обороту наркотиков, совершаемому с использованием информационно- коммуникационных технологий

Нейтрализация противодействия, осуществляемого преступниками при незаконном обороте наркотических средств с использованием различных видов криптовалюты, предполагает совокупность разнообразных мер, к которым возможно отнести следующие.

1. Разработка и внедрение специальных программных продуктов, направленных на деанонимизацию сделок с криптовалютой.

С 2016 г. в мире наблюдается постепенный отказ от использования криптовалюты и внедрение анонимных валют (Dah, Monero, Zcash). Снижение популярности биткойн объясняется тем, что в посреднических транзакциях по типу «человек в середине» Bitcoin позволяет отследить участников сделки и деанонимизировать их через использование общедоступных источников данных.

Так, исследователи из Катарского университета создали методику де-анонимизации сделок с Bitcoin и на ее основе смогли установить личность 22 человек, которые 5 лет назад покупали наркотики на теневом рынке Silk Road.

В конце января 2018 г. разработан сервис Crystal от поставщика блокчейн-решений Bitfury Group, предназначенный для выявления и расследования криминальной деятельности в блокчейне Bitcoin. Сервис позволяет сотрудникам правоохранительных органов и частным экспертам прослеживать пути перемещения подозрительных транзакций до конечного получателя или точки сбыта криптовалюты.

Поскольку технология блокчейн не вызывает полного доверия у государств, ведомств и регуляторов, это порождает различные препятствия к использованию ее как эффективного инструмента взаиморасчетов. В связи с этим специалисты Bitfury Group задумались над тем, чтобы внести в экосистему блокчейна Bitcoin элемент доверия.

По своей архитектуре блокчейн биткойна содержит информацию обо всех транзакциях, и она доступна всем участникам сети. Алгоритмы сервиса Crystal загружают и обновляют данные из блокчей-

на, а также собирают в сети Интернет публично доступную информацию о владельцах кошельков криптовалюты. Вся информация обрабатывается так, чтобы данные в дальнейшем были пригодны для аналитики и могли быть представлены пользователю в удобном формате. Результаты обработки сохраняются. Критериями назначения степени риска являются подтвержденная публичная информация о нелегальной деятельности конкретных участников блокчейна биткойна и наличие транзакций с ними прочих участников, которые формируют так называемый Darknet.

Например, если участник А. взаимодействовал с известным высокорисковым участником В., то участник А. также попадает под «подозрение», т. е. алгоритм присваивает ему некий повышенный уровень риска. Наличие или отсутствие риска отображается в интерфейсе приложения с помощью красных и зеленых меток соответственно. Crystal является аналитическим инструментом и не дает оценок законности транзакций. Считать ту или иную транзакцию сомнительной или незаконной – прерогатива правоохранительных органов.

Отслеживать информацию о транзакциях может либо сам пользователь Crystal, либо сторонняя программа: Crystal содержит API для интеграции с аналитическим ПО пользователя. Сбор персональных данных Crystal не производит.

Разработчики отмечают, что лежащие в основе анализа данных эвристические алгоритмы по своей природе не дают стопроцентного результата. Кроме того, команда проекта выявляет случаи сбоев и постоянно работает над их устранением, улучшая алгоритмы. Поэтому решения, выносимые сервисом Crystal, не являются категоричными – все остается в зоне ответственности пользователя.

Crystal предназначен для двух групп потенциальных пользователей: аналитиков правоохранительных структур, финансовых и страховых компаний, налогового мониторинга, работающих в отделах по борьбе с незаконными финансовыми операциями, и следователей, участвующих в расследовании преступлений, в которых использовался биткойн.

В конце 2018 г. компания Chainalysis, занимающаяся валютными расследованиями, выпустила продукт под названием Know Your Transaction (KYT). Он поможет отслеживать людей, которые участвуют в незаконной деятельности, связанной с криптовалютами. Среди постоянных клиентов Chainalysis – Федеральное бюро расследований США, Администрация по борьбе с наркотиками (DEA) и Европол.

Продукт от KYT от Chainalysis предоставляет обратную связь по транзакциям в реальном времени и отправляет соответствующую информацию на биржу в «движок обработки транзакций». Руководители

площадок видят «рискованных» пользователей и получают возможность отслеживать их подозрительные действия.

Новые виртуальные валюты, в отличие от биткойна, основаны на протоколе с принципом запутывания блоков цепочки, потому установление их владельца, равно как и IP-адреса отправителя, невозможно.

2. Блокировка сайтов, размещающих информацию о продаже наркотических средств.

На сегодняшний день одним способов борьбы с незаконным оборотом наркотических средств в целом и сбытом с использованием криптовалюты в частности является блокировка сайтов Роскомнадзором, который использует схему блокирования либо по IP (адресу интернет-протокола), либо по адресу URL.

Наиболее востребованной социальной сетью среди лиц, относящих себя к членам пронаркотической субкультуры, а также лиц, причастных к распространению наркотиков, является социальная сеть «ВКонтакте», на долю которой в 2018 г. пришлось 6 410 электронных обращений в «Единый реестр», на втором месте – «Одноклассники» (393), далее следует Telegram (293), Facebook (235), Instagram (207), LiveJournal (139) и Twitter (74).

3. Разработка и принятие нормативных положений, направленных на противодействие незаконному обороту наркотических средств, совершенному с использованием криптовалюты.

Проблематика незаконного оборота наркотических средств с использованием криптовалюты требует комплексных мер, в том числе путем проработки соответствующих законодательных инициатив:

1) включения в УК РФ новой бланкетной нормы – ст. 187.1 УК РФ, предусматривающей ответственность за неправомерный оборот криптовалюты (например, «Совершение сделки, связанной с оборотом криптовалюты, в нарушение правил, установленных законодательством РФ, а равно создание и использование компьютерных программ и технических устройств, предназначенных для неправомерного получения доступа к криптовалюте, – наказывается...»);

2) рассмотрения и принятия внесенного в Правительство Российской Федерации проекта федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», направленный на установление ответственности для владельцев интернет-ресурсов, а также хостинг-провайдеров за размещение (распространение) запрещенной информации о наркотических средствах и психотропных веществах, разработанного МВД России совместно с Минкомсвязью России, ФСБ России и Минюстом России.

Резюмируя изложенное, отметим:

а) использование криптовалюты при совершении преступных деяний обусловлено ее свойствами: децентрализацией, анонимностью, трансграничностью и высокой скоростью транзакций; возможностью обмена на другие криптовалюты или фиатные деньги;

б) вытеснение биткойна криптовалютами Dah, Monero, Zcash обусловлено их более высокими конспиративными функциями;

в) отдельными мерами противодействия незаконному обороту наркотических средств с использованием криптовалюты являются: внедрение специальных программных продуктов, направленных на деанонимизацию сделок с криптовалютой (разработанных компаниями Bitfury Group; Chainalysis Know – Your Transaction (KYT), Лондонской Elliptic); блокировка веб-сайтов, размещающих информацию о продаже наркотических средств; внесение изменений и дополнений в отдельные нормативно-правовые акты, а также разработка новых.

Примерный план занятия

1. Субъекты деятельности по борьбе с незаконным оборотом наркотиков.

2. Динамика: выявления преступлений всех видов, в том числе с использованием ИКТ, связанных с незаконным оборотом наркотиков; выявления лиц, совершивших преступления в сфере незаконного оборота наркотиков; выявления преступлений в сфере незаконного оборота наркотиков, совершенных группами лиц; количества наркотиков, изъятых из незаконного оборота правоохранными органами России.

3. Участие органов внутренних дел в проведении ежегодных межведомственных комплексных широкомасштабных оперативно-профилактических операций.

4. Пресечение деятельности организованных преступных группировок, осуществлявших поставки наркотиков в Россию с использованием сети Интернет.

Вопросы для самоконтроля по теме

1. Что понимается под интернет-мониторингом?

2. С использованием каких ОРМ осуществляется интернет-мониторинг?

3. Проблемы, с которыми сталкиваются правоохранные органы, при выявлении и документировании преступлений, связанных с незаконным оборотом наркотиков.

Тема 5.2. Технические возможности использования биллинговых данных при раскрытии и расследовании уголовных дел, связанных с незаконным оборотом наркотиков. Правовая база для использования в раскрытии тяжких и особо тяжких преступлений системы технических средств по обеспечению оперативно-розыскных мероприятий. Понятие и принципы функционирования базовой станции

Возможности информационного взаимодействия между людьми, расширяющиеся по мере развития технологий сотовой связи и сетевой инфраструктуры, используются и в преступных целях, например, для осуществления незаконного оборота наркотических средств и психотропных веществ.

С целью максимального использования возможностей оперативно-технических подразделений ОВД, сотрудники полиции, занимающиеся раскрытием и расследованием уголовных дел, должны понимать принципы организации сотовой связи.

В мире существуют несколько типов сетей цифровой сотовой связи с несовместимыми между собой стандартами связи. К основным стандартам цифровых сотовых сетей можно отнести CDMA (Code Division Multiple Access – множественный доступ с кодовым разделением в настоящее время в Российской Федерации не используется) и GSM (Global System for Mobile Communications – глобальная система связи с мобильными объектами).

В России коммерческая сеть GSM впервые запущена компанией «МТС» в 1994 г. В том же году заработал «Северо-Западный GSM», который позже трансформировался в «Мегафон». Сейчас в России работают четыре крупных оператора сотовой связи: «МТС», «Мегафон», «Билайн» и «Теле2», которые контролируют до 95 процентов рынка услуг сотовой связи, а также порядка 20 мелких региональных компаний, зачастую использующих телекоммуникационное оборудование крупных компаний.

В настоящее время российские операторы сотовой связи работают с сетями сотовой связи 2-го, 3-го и 4-го поколения. Сети сотовой связи 5-го поколения на территории России не развернуты. Распределение частот для различных стандартов и возможные скорости обмена информацией представлены в таблицах.

*Распределение частот для различных стандартов
сетей сотовой связи*

Поколение	800МГц	900МГц	1800 МГц	2100 МГц	2600 МГц
2G		X	X		
3G		X		X	
4G	X	X	X	X	X

*Возможные скорости передачи в информации
в сетях сотовой связи различных поколений*

Предоставляемые услуги	2G	3G	4G	5G
Скорость передачи	до 14 Кб/с	до 2 Мб/с	до 300 Мб/с	до 1 Гб/с

Построение сотовых сетей связи основано на разделении обширной географической зоны обслуживания на участки, называемые сотами, что позволяет осуществлять большое количество звонков (активных соединений) в ограниченном диапазоне радиочастот. При перемещении мобильного телефона от одной соты к другой необходимо обеспечить поддержание активного соединения. Основные компоненты сети: базовая приемопередающая станция (далее – БПС) – приемо-передатчик, который устанавливает связь с мобильными телефонами; контроллер базовой станции (далее – КБС), который управляет приемо-передатчиком и распределяет каналы связи; центр коммутации подвижной связи (далее – ЦКПС), обеспечивающий коммутацию всей сотовой сети (рис. 5.1). КБС и элементы БПС, которыми он управляет, называют подсистемой базовой станции.

Как правило, конфигурация БПС включает в себя три отдельных сектора покрытия по 120 градусов каждый: от 0 градусов к северу до 120 градусов к юго-востоку, от 120 градусов к юго-востоку до 240 градусов к юго-западу и от 240 градусов к юго-западу до 360 градусов к северу (рис. 5.2). Идентификатор соты однозначно определяет БПС и сектор, вовлеченный в обслуживание телефонного вызова.

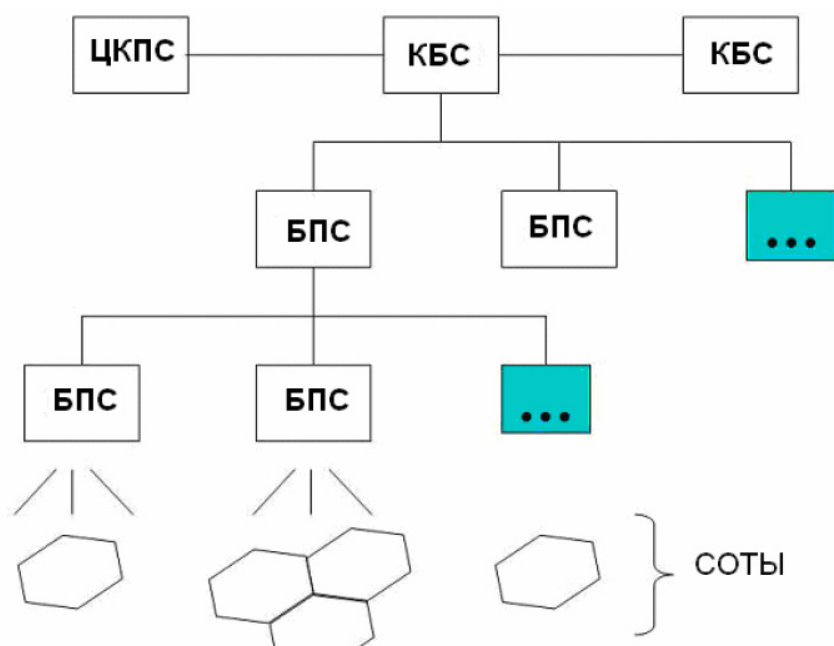


Рис. 5.1. Схема организации сети сотовой связи

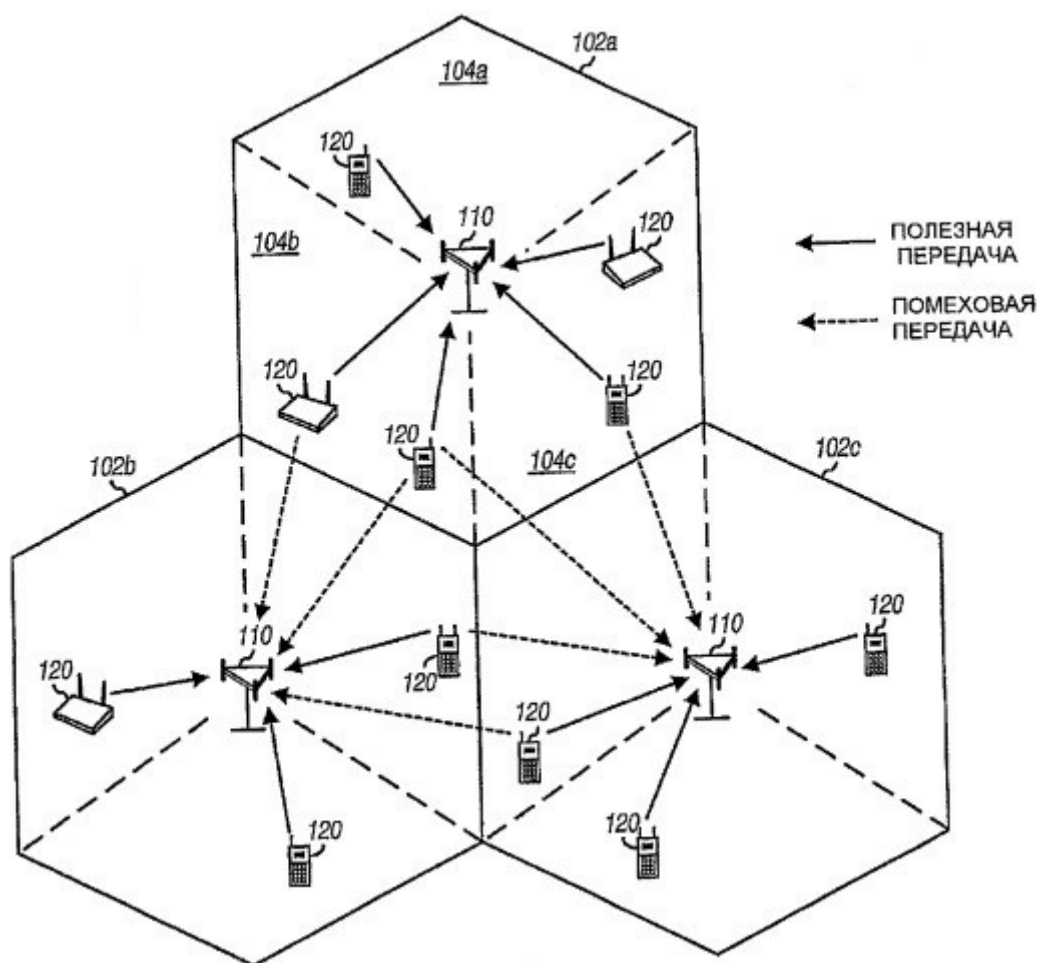


Рис. 5.2. Схема организации базовой станции

Центр коммутации подвижной связи, управляя КБС, руководит всеми коммуникациями в сотовой сети, включая установление связи с коммутируемой телефонной сетью общего пользования. Чтобы выполнять свои задачи, ЦКПС использует несколько баз данных. Главная база данных с информацией об услугах, предоставляемых абоненту, называется регистром местонахождения «домашних» абонентов. Содержащаяся в регистре местонахождения «домашних» абонентов информация об учетных записях (данные об абоненте, предоставляемых услугах, месте последней регистрации в сети), используется центром коммутации подвижной связи для записи информации о звонках. База информации об абонентах и записи информации о звонках являются важным источником доказательств при расследовании преступлений.

Под *биллинговыми данными* понимаются формируемые сетевым оборудованием сведения о стоимости услуг связи, о тарифах и прочих стоимостных характеристиках, а также о технических, временных и пространственных параметрах работы оборудования связи, необходимых для расчета за предоставляемые услуги. Биллинговая информация используется операторами связи для выставления счетов абонентам и взаиморасчетов с другими поставщиками услуг связи.

В ОРД под *биллинговой информацией*, используемой в деятельности правоохранительных органов, понимаются данные о соединениях абонентских терминалов сетей связи (телефонов фиксированной и мобильной связи, средств информационного обмена, модемов и т. д.), в том числе данные о неотвеченных вызовах, об использовании оконечном оборудовании (серийных номерах терминалов (номерах IMEI), справочная информация об абонентах (регистрационные или установочные данные), сведения о приемо-передающем сетевом оборудовании и пространственно-временных характеристиках работы сотовых телефонов (сведения о базовых станциях, через которые осуществлялось соединение абонента), данные о радиотелефонах, работавших в заданных пространственных областях (трафики соединений или «зонты»).

Записи, хранящиеся у поставщика услуг (оператора сотовой связи), содержат информацию, необходимую для того, чтобы точно выставить счет абоненту или, в случае предоплаты, списывать деньги со счета. Эти записи называются записями информации о звонках и создаются при помощи коммутатора, управляющего исходящими звонками и СМС-сообщениями с мобильного телефона. У некоторых поставщиков услуг эти записи могут также включать данные о выде-

ленном канале, станции для коммутации трафика между национальной и международной сетями и информацию о транзакциях. Так как содержимое и формат этих записей могут значительно отличаться у разных операторов сотовой связи, основные данные, необходимые для идентификации абонента (устройства, с которого производится звонок, первоначальная сота, обслуживающая звонок, набранный номер и продолжительность звонка), неизменно фиксируются. Часто сюда включается подробная информация, такая как идентификатор соты (БПС) и сектор.

Помимо записей о звонках, полезную для расследования информацию могут предоставить записи об абоненте, хранящиеся у поставщика услуг, например (в базах данных GSM):

- имя абонента и адрес;
- имя и адрес для выставления счета (если не совпадают с именем и адресом абонента);
- имя пользователя и адрес (если не совпадают с именем и адресом абонента);
- биллинговый счет;
- номер телефона (MSISDN);
- международный идентификатор абонента мобильной связи;
- серийный номер сим-карты (как указано на карте);
- PIN/PUK-код для сим-карты;
- подписанные услуги.

В соответствии с положением п. 1 ст. 64 ФЗ «О связи» операторы связи обязаны хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания таких действий;

2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и обработки.

Пункт 1.1 вышеуказанной статьи обязывает операторов связи предоставлять уполномоченным государственным органам, осуществляющим ОРД или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи, иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных ФЗ.

Порядок предоставления оператором связи уполномоченным государственным органам, осуществляющим ОРД с использованием технических средств, обеспечивающих эту деятельность в сети связи оператора связи, информации об абонентах и оказанных им услугах связи, иной информации, необходимой для выполнения задач, возложенных на данные органы, определен ППРФ от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность» (далее – Правила взаимодействия).

Так, п. 2 Правил взаимодействия определяет, что органы ФСБ осуществляют взаимодействие с операторами связи при проведении ОРМ, связанных с использованием технических средств, кроме всего прочего, в интересах других уполномоченных органов. При отсутствии у органов ФСБ необходимых оперативно-технических возможностей для проведения таких ОРМ, в соответствии с положением п. 3 Правил взаимодействия, указанные ОРМ осуществляют ОВД вместе с тем в интересах других уполномоченных органов.

С целью осуществления ОРМ в каналах связи, в том числе получения биллинговой информации, развернута Автоматизированная информационная система технических средств по обеспечению ОРМ (АИС СОРМ). Она состоит из двух комплектов специальных программно-аппаратных комплексов, один из которых устанавливается у оператора связи, а второй – на территории объекта ОВД, и с его помощью осуществляется управление информационной системой.

При раскрытии и расследовании преступлений в сфере незаконного оборота наркотиков важно помнить о необходимости соблюдения прав и свобод гражданина и человека, законности, режима секретности и конспирации.

Анализ совершенных преступлений в сфере незаконного оборота наркотических средств показывает, что лица, причастные к совершению таких преступлений, активно используют современные средства коммуникации. Совершение такого рода преступлений зачастую подразумевает множественные передвижения причастных лиц с целью перемещения прекурсоров или уже изготовленных наркотических средств, в также с целью их непосредственного сбыта. Как правило, в преступной деятельности используются абонентские номера, оформленные на подставных лиц, а СВТ (телефоны, смартфоны и т. д.) используются ограниченное время (от совершения одного эпизода до нескольких недель), после чего заменяются на новые. Вместе с тем

зачастую преступники имеют при себе и средства связи, используемые в личных целях.

Путем анализа биллинговой информации номера, используемого в преступной деятельности, а также дальнейшего анализа данных базовых станций сети сотовой связи возможно выявление личных номеров. Это дает возможность установления личности преступника, а также может служить доказательством совершения тех или иных деяний.

Процесс получения биллинговых сведений о соединениях абонентов мобильной сотовой связи с указанием базовых станций, их обработка и анализ выглядят следующим образом.

1. По имеющейся информации о месте совершения преступления инициатор запрашивает номер базовой станции, обслуживающей эту территорию (для оформления соответствующего постановления и получения решения суда).

2. Операторам сотовой связи направляется запрос о предоставлении биллинговых сведений о соединениях абонентов за определенный период времени с привязкой к базовой станции и указанием IMEI абонентов.

3. Оператор предоставляет биллинг в следующем виде: тип учетной записи, номер телефона абонента А, набранная последовательность абонента Б, дата и время начала соединения, продолжительность, IMEI, данные базовой станции абонента А (в начале разговора), данные базовой станции абонента А (в конце разговора), данные базовой станции абонента Б (в начале разговора), данные базовой станции абонента А (в конце разговора).

4. Выполняется поиск совпадений по месту и времени.

5. Проводится ориентирование оперативных подразделений на проведение действий в отношении выявленных абонентов, возможно причастных к совершению преступления.

Примерный план занятия

1. Технические возможности использования биллинговых данных при раскрытии и расследовании уголовных дел, связанных с незаконным оборотом наркотиков.

2. Правовая база для использования в раскрытии тяжких и особо тяжких преступлений системы технических средств по обеспечению ОРМ.

3. Понятие и принципы функционирования базовой станции.

Вопросы для самоконтроля по теме

1. Что понимается под биллинговыми данными в сфере электро-связи?
2. Что понимается под биллинговой информацией в оперативно-разыскной деятельности?
3. Назначение центра коммутации подвижной связи.
4. Назначение базовой приемопередающей станции.
5. Какую информацию об абонентах могут предоставить поставщики услуг?
6. Возможности использования биллинга при раскрытии и расследовании преступлений в сфере оборота наркотиков.

Тема 5.3. Тактика противодействия незаконным наркооперациям, совершаемым с использованием блокчейн-технологий

Сущность незаконного сбыта с использованием интернет-технологий предполагает отсутствие личного контакта и высокий уровень конспирации как в процессе приобретения наркотических средств, так и при взаимодействии участников преступной группы (сообщества), численность которых в крупных интернет-магазинах (например, «КВЕСТ», Stuff.store, «ХимПром», «Хэппи Лэнд», Express, ХТС) может достигать до нескольких сотен: закладчиков, операторов, кассиров, курьеров, менеджеров по регионам, финансовых директоров, специалистов в области информационной безопасности. Оплата за приобретенные наркотические средства, а также начисление заработка участникам преступного сообщества осуществляется с использованием электронных платежных систем на банковские карты, оформленные на подставных лиц.

Для обозначения интернет-ресурсов, используемых для незаконного распространения наркотических средств, в литературе употребляются понятия Darknet, «Темный интернет», TOR.

На территории России и ряда стран СНГ с конца октября 2016 г. функционирует крупнейшая торговая площадка Gidra (400 интернет-магазинов). Структура указанного TOR-сайта схожа с аналогичными ресурсами, действующими в США. Сделки и оплата происходят непосредственно на площадке. Оплата – исключительно в криптовалюте биткойн, не связанной с централизованными платежными системами, а потому неподконтрольной каким-либо органам власти. Это исключает возможность обнаружения и изъятия денежных средств (в том числе и с индивидуальными признаками, используемых сотрудниками правоохранительных органов в ходе проведения ОРМ), получаемых участниками преступного сообщества (преступной организации), и обеспечивает анонимность участников преступного сообщества (преступной организации), а также покупателей наркотиков. Площадка охватывает все сферы теневого бизнеса: от продажи наркотических средств до торговли поддельными документами, банковскими картами, специальным оборудованием для слежки

и съема информации, а также предоставляет различные информационные услуги.

С октября 2017 г. по март 2018 г. на площадке Gidra размещался анонимный автоматизированный интернет-магазин «КВЕСТ» по продаже наркотических средств, психотропных веществ и частей растений, содержащих наркотические средства. Доступ к нему был возможен исключительно посредством интернет-браузера TOR, что не позволяло идентифицировать интернет-пользователя, обеспечивая тем самым безопасность незаконных операций, связанных с незаконным сбытом наркотиков.

Криптовалюта функционирует на основе блокчейна, представляющего собой базу данных, которая хранит информацию обо всех транзакциях участников системы в виде цепочки блоков. Уникальность блокчейна заключается в неизменности или необратимости, которую гарантирует криптографическая система защиты. Тем самым блокчейн обеспечивает одновременно высокую степень защиты данных, с которыми работают пользователи, и прозрачность транзакций для системного контроля.

Пользователи криптовалюты владеют ключами, которые закрепляют права владения в транзакциях блокчейна, разрешая производить трату средств и перемещать их новому владельцу. Эти ключи обычно хранятся в онлайн-кошельках на компьютерах авторизованных пользователей. Владение ключами является единственным необходимым требованием для создания и осуществления транзакций. Следовательно, вся ответственность и контроль над средствами перекладываются на самих пользователей.

Схема перемещение средств в блокчейне показана на рисунке 5.3.



Рис. 5.3. Схема перемещения средств в блокчейне

Процесс ускоренного интегрирования криптовалюты в незаконный оборот наркотических средств объясняется ее основными свойствами.

1. Децентрализацией (отсутствием главного сервера, который бы контролировал все операции).

2. Трансграничностью и транснациональностью.

3. Обеспечением анонимности сделок. В отдельных альтернативных платежных системах используются специальные технологические решения (например, так называемые миксеры), которые препятствуют идентификации криптовалютных транзакций и их участников. Это позволяет скрывать личности отправителей и получателей криптовалюты, утаивать содержание операций и практически исключает контроль правоохранительных и финансовых органов за движением платежных средств, представленных криптовалютой.

4. Совершением транзакций в режиме P2P: равенство пользователей, транзакции осуществляются напрямую при отсутствии посредников.

5. Высокой скоростью обработки транзакций.

6. Отсутствием банковского, валютно-экспертного и налогового контроля, а также обязательного контроля, предусмотренного системой противодействия отмыванию доходов и финансированию терроризма и незаконному обороту наркотических средств. В большинстве альтернативных платежных систем транзакции проверяются лишь на соответствие системному протоколу (валидация) при отсутствии механизмов их проверки на предмет соответствия законодательству.

7. Использованием криптовалюты в качестве мобильного средства сбережения. «Приватные» ключи, эквивалентные сотням миллионов долларов, можно хранить на крошечном USB-накопителе и легко переносить в любое место.

8. Возможностью обмена на другие криптовалюты или фиатные деньги.

Примерный план занятия

1. Потоки денежных средств от наркопотребителей к организаторам.

2. Финансирование незаконной деятельности.

3. Состав преступных сообществ.

4. Использование криптовалют в сетевом сбыте наркотиков.

5. Использование электронных средств платежа в сетевом сбыте наркотиков.

6. Механизмы расчетов, наиболее часто используемые за наркотические средства и легализации доходов.

Вопросы для самоконтроля по теме

1. В чем заключается уникальность блокчейна?

2. Использование какого интернет-браузера не позволяет идентифицировать интернет-пользователя?

3. Какими свойствами объясняется процесс интегрирования криптовалюты в незаконный оборот наркотических средств?

Тема 5.4. Особенности раскрытия преступлений в сфере оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий

В настоящее время сбыт наркотических средств и психотропных веществ, осуществляемый бесконтактным способом посредством сети Интернет, носит поистине массовый характер. Использование наркопреступниками сети Интернет, средств мобильной связи и электронных платежей делает выявление такого рода преступлений чрезвычайно затратными и трудоемкими, а возможности оперативных сотрудников не позволяют должным образом осуществить документирование продажи наркотических средств ОПГ, специализирующимися на их реализации бесконтактным способом. Данные группы носят межрегиональный или межгосударственный характер, что также существенно затрудняет процесс выявления такого рода преступлений. Сетевой структуре ОПГ присуща высокая живучесть за счет способности подстраиваться под изменения законодательства в сфере незаконного оборота наркотических средств и тактических приемов выявления преступлений, а также избирать наиболее оптимальные и высокотехнологичные способы общения участников ОПГ и наркопотребителей, получения денежных средств.

Зачастую в ходе ОРМ, направленных на документирование преступной деятельности сбытчиков, к уголовной ответственности удается привлечь лишь рядовое звено наркопотребителей, в то время как непосредственные организаторы избегают заслуженного наказания.

В связи со способностью ОПГ адаптироваться к изменению нормативно-правовой базы, необходимо признать, что противодействие наркопреступности на законодательном уровне за последние несколько лет не привело к каким-либо значимым результатам. Так, в целях совершенствования механизма отнесения того или иного вещества к запрещенным была введена новая ст. 234.1 УК РФ с пакетом соответствующих поправок в УПК РФ и КоАП РФ. Органы наркоконтроля наделялись особым правом оперативно запрещать оборот любого потенциально опасного вещества, воздействие которого на организм по первичным признакам схоже с наркотическим.

До настоящего времени указанные нормы на территории России практически не реализуются, и это при том, что новые потенциально опасные вещества с измененной формулой регулярно появляются на наркорынке.

Отправной точкой в организации сети сбыта наркотических средств является создание «организатором» специального сетевого ресурса в сети Интернет. Он может носить форму автоматизированного сайта или отдельной страницы на каком-либо интернет-форуме. Обычно для таких целей используют уже существующие на протяжении длительного времени сайты с устоявшимся именем, где путем присоединения «организатор» может разместить свою информацию: рекламу наркотических средств, их стоимость, систему оплаты и возможные варианты передачи запрещенных веществ. Нередко сетевые ресурсы такого рода создаются на серверах, расположенных в других странах, что обеспечивает им дополнительную конспирацию. Специфика организации и деятельности таких ресурсов давно уже перешла из разряда единичных, автономно используемых, в категорию системно организованных, объединенных и хорошо координируемых в интернет-пространстве. Лица, участвующие в этом процессе, могут находиться и за рубежом, используя специальные приемы, делающие затруднительным их обнаружение, в частности использование так называемых ботов в качестве администраторов сайта.

Дилер выступает в роли руководителя остальных членов группы, которая создается по мере продвижения рекламы и сбыта наркотических средств. Его роль сводится к непосредственному использованию информационных возможностей интернет-ресурса, приобретению, фасовке крупных партий спайса, разработке схемы по получению и перемещению денег. Он также договаривается с производителями и поставщиками наркотических средств. В случае необходимости дилером привлекается к участию так называемый региональный менеджер с аналогичными функциями, отвечающий за организацию сбыта наркотических средств в отдельном регионе.

Производитель синтезирует или выращивает наркотические средства, прячет их оптовые партии и передает их адреса оператору.

Роль поставщика заключается в получении заказов на доставку наркотических средств с владельцев магазинов, найме дропов (подставное лицо, участвующее в преступных схемах с наибольшими рисками, например в обналичивании денежных средств в банкоматах, получении посылок и др.), получении от дропов адресов спрятанного товара, перезакладке его и отправлении магазину координат.

Необходимым условием развития наркосети является налаживание информирования. Как правило, информационные сайты ОПГ обладают всеми атрибутами интернет-магазинов с представительствами в субъектах Российской Федерации, а зачастую и в странах ближнего

зарубежья: прайс-листом с оговоренными скидками, контактами с продавцом (по шифрованным каналам), курьерской службой, клиентской базой и пользовательским форумом, участники которого делятся мнением о работе «магазина» и качестве «товара». Над продвижением сбыта работают специально нанятые рекламщики, использующие как интернет-ресурсы, так и примитивную городскую рекламу в виде трафаретных надписей на стенах зданий, тротуарах.

Ключевой ролью в ОПГ обладает оператор, в задачи которого входит внесение большого депозита дилеру, наем курьеров для доставки товара от поставщиков до складменов (кладовщиков), передача складменам адресов оптовых партий, передача адресов для закладок кладменам (закладчикам), размещение адресов подтвержденных кладов в базе моментальных магазинов, контроль продаж. Он также ведет переписку с клиентами (например, в XMPP), разбирается от лица магазина по поводам обнаружения покупателемклада в условленном месте.

Необходимым звеном ОПГ является курьер. В зависимости от объема продаваемого наркотического средства и географии группы курьеров может быть до десяти и более. В их обязанности входит расфасовка на мелкие партии получаемых наркотических средств, закладка их в тайники и передача информации об их местоположении оператору.

Следует отметить конспиративность данной схемы практически на всех этапах: заказа на интернет-странице у оператора, обезличенного перечисления денежных средств путем электронного платежа, получения адреса места закладки наркотических средств. Все участники купли-продажи наркотических средств остаются анонимными друг для друга.

Вербовка новых участников группы, как правило, проходит через форум Работа интернет-магазина, где аккумулированы региональные вакансии и резюме соискателей, зачастую содержащие фотографию паспорта, подробную анкету, информацию об автомобиле. При документировании преступной деятельности ОПГ такие листы учета кадров помогают выяснить полную картину вовлеченных в наркобизнес лиц.

На интернет-площадках администрацией обеспечивается так называемое страхование сделок в связи с предоплатой товара.

Первый способ страхования – это квоты дилеров (базовая, продвинутая и на специальные товары), дающие право вести торговлю на ресурсе. Они приобретаются у администрации и могут быть аннули-

рованы за нарушение правил торговли. Второй способ – внесение дилерами депозитов, которые хранятся администрацией площадки. Как правило, чем выше товарооборот дилера, тем выше депозит.

Третий способ страхования – созданная администрацией система гаранта. Магазины отвечают за товар в течение 12 часов после заказа: если покупатель купил клад с гарантом и не нашел его, то он открывает диспут – разбирательство с привлечением администратора торговой площадки. Он изучает представленные клиентом, кладменом и представителем магазина фотографии и аргументы, после чего нередко назначает перезаклад, т. е. покупателю отправляется другой адрес местонахождения наркотических средств. Стоимость перезаклада вычитается из залога кладмена.

Процесс выявления преступной деятельности необходимо начинать с системного мониторинга сетевых ресурсов, предлагающих запрещенные вещества, средствами поисковых сервисов. Такой мониторинг позволяет сотрудникам оперативных подразделений обнаруживать интернет-магазины, осуществляющие незаконный оборот наркотических средств, затем через электронное обращение направлять материалы в Роскомнадзор и впоследствии блокировать такие ресурсы на уровне провайдеров. Исключение ссылок на криминальные интернет-ресурсы – профилактическое и подрывающее противоправный бизнес воздействие.

Однако этот способ является трудозатратным, длительным и зависящим от человеческого фактора; в условиях массового доступа к Интернету, высокой динамичности информационных процессов в нем невозможно оперативно отслеживать электронные торговые площадки и блокировать ресурсы, содержащие противоправный контент.

Для более эффективного выявления преступлений необходимо использование автоматизированных систем мониторинга интернет-ресурсов, а для блокирования доступа пользователей Интернета к противоправному контенту требуется более активное содействие отечественных поисковых сервисов (Yandex, Rambler, Mail).

Кроме предупредительных и профилактических мер, правоохранительные органы реализуют и другие мероприятия по раскрытию преступлений, совершаемых посредством сети Интернет. Следующим этапом после выявления факта сбыта наркотических средств посредством сети Интернет является обнаружение СВТ, с помощью которых осуществлялись противоправные действия или которыми пользовались злоумышленники в качестве средств коммуникации. Основным идентифицирующим признаком сетевого интерфейса СВТ

в Интернете является его IP-адрес, назначаемый интернет-провайдером абонента, а также MAC-адрес (физический адрес), оформляемый производителем оборудования, так же известный интернет-провайдеру. Следовательно, установление IP-адреса устройства позволяет определить местоположение абонента и получить возможность документировать сеансы его соединения и содержание передаваемой информации как доказательства факта совершения лицом преступных действий. Такая задача может решаться, например, в рамках ОРМ «Получение компьютерной информации» и «Снятие информации с технических каналов связи».

Трудности в этом вопросе возникают из-за использования преступными группами средств анонимизации (например, преобразование сетевых адресов (NAT)), позволяющих скрывать цепочку адресов маршрута соединения, и шифрования трафика методами криптографии. Относительную прозрачность сетевых адресов и объемов трафика обеспечивает внедряемый с 2012 г. интернет-протокол Ipv6, однако сейчас его доля использования не превышает 30%, многие сетевые устройства его не поддерживают. Вторым решением проблемы является тотальное проведение на каналах провайдеров ОРМ на основе применения систем глубокого анализа трафика DeepPacketInspection, способных мгновенно анализировать стационарные и потоковые данные на всех уровнях сетевой модели OSI. Эти же системы можно применять для мониторинга контента, передаваемого или хранимого на интернет-ресурсах.

Сеть Tor не является абсолютно анонимной, в Интернете публикуются уязвимости, связанные с существованием контролируемых узлов, транслирующих трафик, и открытости данных, передаваемых от последней цепочки в соединении. В Интернете неоднократно обсуждалась схема отслеживания коммутационной цепочки пакетов Tor на основе timing-атаки или выявления паттерна трафика (статистической зависимости объема трафика от времени), когда анализируется время прохождения пакетов и устанавливается маршрут их движения по сети. Но такие возможности могут быть реализованы только в условиях контроля большого количества маршрутизаторов сети Интернет.

Для получения значимой в интересах раскрытия преступлений информации важна целенаправленная работа с интернет-компаниями. Источниками информации о пользователях сети могут являться компании, предоставляющие различные интернет-услуги (телекоммуникация, форумы, социальные сети, хостинг и др.). Существенную про-

блему в установлении IP-адреса абонента и иной оперативно значимой информации составляют зарубежные интернет-компании: в отсутствие юрисдикции законов нашего государства на территории другой страны взаимодействие с иностранными сервисами практически не осуществляется, интерес в сотрудничестве у западных спецслужб отсутствует, поэтому проведение отдельных видов ОРМ становится невозможным. Можно допустить активные формы борьбы с бесконтактным сбытом наркотических средств, связанные с использованием хакерских методов и вирусоподобного ПО. Это даст возможность напрямую воздействовать на источники противоправной информации или компьютерные средства фигурантов незаконного бизнеса. Такие действия требуют юридического сопровождения.

Необходимо представлять изначально, какую оперативно значимую информацию требуется получить и возможно ли это технически (выбор и тактика применения в ОРМ специальной аппаратуры, корректность заданий для ПСТМ), а для этого – обладать специальными техническими знаниями.

Наравне с техническими мероприятиями оперативные сотрудники реализуют методы получения информации о фигурантах преступлений в открытых источниках (например, перехват восстановления пароля аккаунта, «засвечивание» телефона в социальной сети и др.). Эффективным средством деанонимизации пользователей могут служить различные http-снифферы, программные закладки, специальное ПО и др. Перспективным направлением является анализ связей пользователей в социальных сетях.

Участники ОПГ по сбыту наркотических средств используют электронные платежные системы и криптовалюты для легализации и транзакций денежных средств. Компании платежных систем имеют в своем распоряжении средства автоматизированной аналитической обработки транзакций по своим счетам и построения на этой основе графических схем финансовых потоков, но в рамках ОРМ доступа к ним оперативные сотрудники не получают. Чаще всего в незаконном обороте наркотических средств в силу своей доступности и популярности используются QIWI-кошельки. При анализе информации QIWI-кошельков транзакции по счету, который задействован в незаконном сбыте, выстраивают в граф, отследить движение денежных средств далее по связанным счетам возможно только последовательно в силу законодательных норм.

В расчетах криптовалютами типа биткойн, в которых при отсутствии центрального узла учета деньги хранятся на кошельках вла-

дельцев в зашифрованном виде, все транзакции адресно анонимны и невозможно установить владельца кошелька. Однако для вывода денег на монетизируемые счета пользователи используют различные обменники и интернет-биржи. Контроль биржевых операций со стороны правоохранительных органов мог бы решить некоторые проблемы выявления преступных финансовых схем. Не следует недооценивать возможности компьютерно-технической экспертизы, так как действия пользователя сохраняются на компьютере в виде журнала событий, сообщений, списка посещенных интернет-страниц, удаленных файлов, резервных копий, аккаунтов и др. В случае обнаружения с помощью специализированных программ кошельков криптовалют на компьютерных устройствах возможно реальное отслеживание всех транзакций, в которых они фигурируют.

Методами ОРД возможно выявление фактов сбыта наркотических средств путем интернет-продаж по информации от наркопотребителей о закладчике, вероятных местах хранения наркотических средств, характерных приемах конспирации. На основе анализа такой информации разрабатываются ОРМ, направленные на установление личности закладчика.

После установления всех участников группы, осуществленного с применением комплекса ОРМ, производится оценка полученных оперативных материалов, в том числе с участием сотрудников следственных органов. Если на первоначальных этапах документирования возбуждается уголовное дело, это ускоряет проведение всех необходимых оперативно-следственных действий (задержания фигурантов, обыска, выемки, допроса и др.).

Вопросы для самостоятельного изучения

1. Понятие сетевого трафика.
2. Сетевая модель OSI.
3. Формирование и формат сетевого адреса.

Примерный план занятия

1. Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых с использованием ИКТ.
2. Виды преступлений, совершаемых с использованием ИКТ. Современные способы их выявления и раскрытия.

3. Своевременное получение необходимой информации как один из основных элементов в ходе раскрытия преступлений в сфере незаконного оборота наркотиков.

Вопросы для самоконтроля по теме

1. Участники преступных групп, совершаемые преступления в сфере НОН с использованием ИКТ.

2. Схемы легализации и вывода денег с использованием электронных платежных систем или криптовалют.

3. Алгоритм действий, направленный на документирование ОПГ, специализирующихся на сбыте наркотических средств

Тема 5.5. Взаимодействие оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании преступлений по линии незаконного оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий

Согласно официальным данным Генеральной прокуратуры России, зарегистрировано преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ или их аналогов, в 2017 г. – 208 681, в 2018 г. – 200 306, в 2019 г. – 190 197, в 2020 г. – 189 905, в 2021 г. – 179 732, в 2022 г. (по апрель) – 60 555.

Выявлено лиц, совершивших наркопреступления: в 2017 г. – 106 258, в 2018 г. – 95 683, в 2019 г. – 85 425, в 2020 г. – 83 137, в 2021 г. – 85 147, в 2022 г. (по апрель) – 28 660¹.

Значительное количество подобных преступлений совершается с использованием ИКТ, в частности сети Интернет.

При осуществлении органами полиции экспертно-криминалистической деятельности проводится ряд криминалистических исследований (экспертиз) по противодействию незаконному обороту наркотиков. Следственные действия и ОРМ в данной сфере обладают особенностями. Формы взаимодействия оперативных и экспертно-криминалистических подразделений обусловлены объемом и содержанием следственных действий и ОРМ. Следователь определяет целесообразность привлечения специалиста-криминалиста к тому или иному следственному действию, руководствуясь ст. 168 УПК РФ «Участие специалиста»², с учетом конкретной ситуации.

В ходе расследования преступлений, связанных с незаконным оборотом наркотических средств и их аналогов, осуществляемых с использованием сети Интернет, следует учитывать, что, как правило, они совершаются молодыми людьми, ранее осужденными за совершение аналогичных преступлений, не имеющими какого-либо источника доходов, но обладающими определенными знаниями в области ИКТ, позволяющими использовать им СБТ и ПО в достижении своих преступных целей. Развитие ИКТ привело к тому, что на практике потребитель и сбытчик наркотиков крайне редко знают друг друга в лицо. Технология закладок основывается на использовании таких ин-

¹ Портал правовой статистики Генеральной прокуратуры России. URL: http://crimestat.ru/offenses_chart (дата обращения: 08.06.2022)

² Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в ред. от 01.07.2021). Доступ из справ.-правовой системы «Гарант».

тернет-ресурсов как «Телеграмм», Hydra, AivaShop Darknet, которые обеспечивают высокий уровень конспирации участников операций по сбыту наркотиков и их переговоров.

В настоящее время существует большое количество программ, способных скрыть IP-адрес СБТ. К ним относится, например, программа Orbot, используемая как на стационарных, так и мобильных СБТ. Orbot обеспечивает:

- конфиденциальность (за счет скрытия IP-адреса) пользователя интернет-ресурса и обращения к нему;
- доступ к заблокированному контенту за счет подмены IP-адреса пользователя;
- сокрытие цифровых следов.

Цифровые следы – это данные о действиях пользователя в Интернете. Речь может идти как о «пассивных», так и об «активных» следах, которые остаются при размещении каких-либо сведений о себе в Интернете (к примеру, на сайтах или в социальных сетях). Если скрыть IP-адрес, то «пассивные» следы практически не обнаружимы.

При использовании подобных программ IP-адрес, по которому определяется не только устройство, с которого был осуществлен выход в сеть Интернет, но и местонахождение данного устройства, через определенное время меняет номер IP-адреса и место дислокации, вплоть до другого конца Земли, хотя фактическое место дислокации пользователя при этом не меняется. Orbot обладает функцией шифрования информации и изображений при их передаче по сети второму лицу, что исключает использование данной информации в качестве доказательства по уголовному делу.

При задержании лиц, в действиях которых усматриваются признаки состава преступления, связанного с незаконным оборотом наркотических средств, следователю рекомендуется предпринять все необходимые действия и меры для обнаружения и фиксации доказательств, выражающихся в способах и различных путях незаконного приобретения и сбыта наркотических веществ с использованием сети Интернет. Необходимо обратить внимание на наличие программ, способных скрывать IP-адрес, местоположение устройства и шифровать передаваемую информацию.

Объектом поиска является информация, отражающая умысел злоумышленника – незаконное приобретение или сбыт наркотических средств, психотропных или сильнодействующих веществ и их аналогов:

– переписка лица, приобретающего наркотическое средство, с лицом, незаконно сбывающим такие средства (подобная информация может содержаться в СМС-сообщениях, а также в различных социальных сетях, таких как «ВКонтакте», «Телеграмм», ICQ и т. д.;

– номера телефонов, содержащихся в списке телефонной книги и журнале вызовов;

– паспортные и иные данные, такие как номера банковских счетов, электронных денежных кошельков QIWI, «Яндекс.Деньги», PayPal, для совершения денежных переводов;

– иная информация, распространяемая через Интернет, имеющая значение для уголовного дела, которая подтверждает направленность умысла лица – незаконное распространение или приобретение наркотических средств.

По прибытии на место производства следственного действия необходимо незамедлительно принять меры к обеспечению сохранности СВТ и содержащейся в них информации.

При осмотре мест происшествий, связанных с использованием средств сотовой связи следователю необходимо привлекать специалистов, обладающих специальными познаниями и владением специальным программным и аппаратным инструментарием для извлечения интересующей следствие информации из мобильных СВТ в ходе проведения следственных действий.

Обнаруженная информация позволяет:

– получить сведения об интересующем устройстве сотовой связи;

– выявить круг общения определенного лица, соучастников преступления;

– выявить характер взаимоотношений определенных лиц;

– определить дислокацию конкретного лица;

– получить текстовую информацию, аудиозаписи, фото- и видеоизображения определенного лица.

Компьютерная экспертиза вышла на первый план по значимости по отношению к другим инженерно-техническим экспертизам (в области автоматизации, радиотехники, электроники, электротехники и др.). К судебной компьютерно-технической экспертизе относят следующие виды экспертиз¹:

– информационно-компьютерная экспертиза;

¹ Криминалистическая экспертиза мобильных устройств – порядок проведения. URL: <https://codeby.net/threads/kriminalisticheskaja-ehkspertiza-mobilnyx-ustrojstvporjadok-provedenija.67695> (дата обращения: 11.03.2021).

- аппаратно-компьютерная экспертиза;
- программно-компьютерная экспертиза;
- компьютерно-сетевая экспертиза.

Информационно-компьютерная экспертиза решает вопросы диагностики, идентификации и анализа информации, содержащейся в памяти исследуемого устройства.

Аппаратно-компьютерная экспертиза направлена на всестороннее исследование материальных носителей информации, включая их происхождение и условия эксплуатации.

Программно-компьютерная экспертиза изучает назначение и состояние ПО, а также обусловленные им функциональные особенности устройства, представленного на исследование.

Компьютерно-сетевая экспертиза назначается в отношении сетей и телекоммуникационных технологий, объектами ее изучения могут быть технические каналы связи, интернет-сервисы (например, электронная почта), интернет-технологии, аппаратура сотовой связи, ресурсы сетевых провайдеров и др.

Все перечисленные компьютерно-технические экспертизы производятся комплексно и последовательно, так как исследуются по большей части целостные компьютерные системы устройства сотовой связи или часть таковой.

В процессе исследования мобильного телефона или планшета перед экспертом ставятся следующие вопросы:

- установлено ли на исследуемом объекте мобильное приложение WhatsApp (Viber, Telegram и т. д.);
- имеется ли возможность установить дословное содержание переписки в мобильном приложении WhatsApp (Viber, Telegram и т. д.) исследуемого объекта с контактом;
- идентична ли переписка, содержащаяся в мобильном приложении WhatsApp (Viber, Telegram и т. д.), переписке, указанной в протоколе (содержание, дата и время отправки и получения сообщений, адресаты сообщений);
- можно ли сделать определенный вывод об отправке, получении и прочтении абонентами данных сообщений за указанные даты и время;
- имеются ли признаки фальсификации, модификации указанных сообщений с использованием специальных программ, иных средств и способов (изменения содержания, подмена отправителя и (или) получателя, изменение даты и (или) времени, искусственного

создания неотправленных и неполученных сообщений под видом отправленных и полученных);

- имеются ли требуемые файлы (фото, видео или др.) в файловой системе представленного на экспертизу мобильного телефона (планшета).

На основании ст. 87, 88 УПК РФ следователь соотносит полученную информацию с имевшейся ранее, анализирует источники происхождения информации, при необходимости производит следственные действия, направленные на получение доказательств, которые могут либо подтвердить полученную компьютерной экспертизой информацию, либо ее опровергнуть.

Информацию, полученную из устройств сотовой связи, можно использовать для производства следственных действий (предъявления для опознания, допроса, обыска и задержания, контроля и записи телефонных переговоров и др.). Большое значение применение такой информации имеет в расследовании преступлений по горячим следам.

Данные абонентов связи при их регистрации, хранящиеся не менее 3 лет в базах данных оператора сотовой связи, фиксация контакта абонента с базовыми станциями могут эффективно использоваться в целях розыска преступников.

В розыске лиц важную роль играют:

- данные активированных карт экспресс-оплаты;
- персональная информация пользователя устройства;
- установление базовой станции оператора сотовой связи, задействованной при совершении преступления.

Специальные знания в экспертно-криминалистическом обеспечении раскрытия и расследования преступлений данной категории могут использоваться в формах:

- 1) производства судебных экспертиз в расследовании преступлений, связанных с незаконным оборотом наркотиков;
- 2) участия специалистов в следственных действиях и ОРМ;
- 3) консультаций;
- 4) технического содействия;
- 5) профилактической работы специалиста;
- 6) обучения специалистом следователей и оперативных сотрудников применению технических средств¹.

¹ Наурызбаев Е.А., Култасов А.А., Нукиев Б.А. Исследовательская деятельность в борьбе с незаконным оборотом наркотиков. Кокшетау: Кокшетауский гос. ун-т им. Ш. Уалиханова, 2017. С. 120–125.

Участие специалиста в проведении ОРМ является факультативным и может представлять собой:

- консультации и обучение оперативных сотрудников навыкам применения технических средств;
- исследование различных вещественных объектов в целях выявления криминалистических признаков, имеющих значение для раскрытия преступления и установления преступников;
- составление розыскных таблиц с использованием криминалистической информации о лицах, предметах и т. д.;
- изготовление субъективных портретов неустановленных преступников;
- сбор идентификационной информации для отождествления личности;
- оказание помощи в отборе образцов для сравнительного исследования;
- участие в разработке розыскных версий на основании криминалистического изучения следов и вещественных доказательств;
- использование экспертно-криминалистических картотек и коллекций.

Примерный план занятия

1. Правовые основы взаимодействия оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании наркопреступлений, совершаемых с использованием ИКТ.

2. Применение экспертно-криминалистических средств и методов при проведении отдельных видов следственных действий и ОРМ.

3. Особенности назначения криминалистических исследований (экспертиз) при раскрытии и расследовании преступлений, совершаемых с использованием ИКТ.

4. Тактика назначения судебных экспертиз при расследовании преступлений, связанных с незаконным оборотом наркотиков.

Вопросы для самоконтроля по теме

1. Что представляет из себя программа Orbot?
2. Перечислите вопросы, которые ставятся перед экспертом в процессе исследования мобильного телефона или планшета.
3. Какие формы взаимодействия оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании преступлений по линии незаконного оборота наркотиков вы знаете?

Перечень нормативных правовых актов, основной и дополнительной учебной литературы

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993.
2. Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 18.12.2001 № 177-ФЗ. Доступ из справ. правовой системы «Гарант».
3. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ. Там же.
4. О полиции: федер. закон от 7.02.2011 № 3-ФЗ. Там же.
5. О государственной судебно-экспертной деятельности в Российской Федерации: федер. закон от 31.05.2001 № 73-ФЗ. Там же.
6. Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность: постановление Правительства РФ от 27.08.2005 № 538. Там же.
7. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного суда Российской Федерации от 30.11.2017 № 48. Там же.

Основная литература

1. Методы и способы получения доказательственной информации с электронных носителей: курс лекций / сост. А.В. Скачко. – Краснодар: Краснодар. ун-т МВД России, 2014. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
2. Баркалова Ю.М Подготовка экспертов по производству компьютерных судебных экспертиз: метод. рекомендации. Воронеж: Воронежский институт МВД России, 2013. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
3. Криминалистика: учеб. / ред. А.Г. Филиппов. 3-е изд., перераб. и доп. М.: Юрайт, 2013.
4. Криминалистика. Углубленный курс: учеб. / ред. А.Г. Филиппов. М.: ДГСК МВД России, 2012.
5. Справочник следователя. Осмотр места происшествия / сост. А.В. Боловинов и др. М.: ЦОКР МВД России, 2010.

Дополнительная литература

1. Введенская О.Ю. Информационно-телекоммуникационная сеть Интернет как источник следовой информации о криминальном событии: фондовая лекция. Краснодар, КрУ МВД России, 2016. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

2. Еремченко В.И., Зиновьева Н.С., Алексеенко И.Л. Юридические и организационные аспекты использования информационно-телекоммуникационных систем в целях противодействия экстремистской деятельности в современных условиях: науч.-практ. пособие. Краснодар: Краснод. ун-т МВД России, 2015.

3. Першин А.Н. Криминалистические основы анализа документированной информации в уголовном судопроизводстве. Омск: Омская академия МВД России, 2015. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

4. Стельмах В.Ю. Получение информации о соединениях между абонентами и(или) абонентскими устройствами как следственное действие. Екатеринбург: Уральский юридический институт МВД России, 2014. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>

5. Судебные экспертизы в гражданском судопроизводстве: организация и практика: науч.-практ. пособие / ред. Е. Р. Россинская. М.: Юрайт, 2011.

6. Тактика следственных действий, направленных на отыскание, обнаружение и исследование электронных носителей и информации на них: учеб. пособие / ред.: А.А. Кузнецов, Д.В. Муленков. Омск: Омская академия МВД России, 2015.

7. Олейник Н.А., Медведчук А.А. Взаимодействие следователя, оперативного работника и эксперта-криминалиста при раскрытии и расследовании преступлений, связанных с незаконным оборотом наркотиков. Курск: Региональный открытый социальный институт, 2018.

8. Селезнев В.М. Роль судебных экспертиз и функции эксперта при расследовании преступлений, связанных с использованием устройств сотовой связи // Современные технологии в юриспруденции: применение специальных познаний. Красноярск: Красноярский государственный аграрный университет, 2021. С. 83–88.

9. Криминалистическая экспертиза мобильных устройств – порядок проведения. URL: <https://codeby.net/threads/kriminalisticheskaja->

ehkspertiza-mobilnyx-ustrojstvporjadok-provedenija.67695 (дата обращения: 11.03.2021).

10. Наурызбаев Е.А., Култасов А.А, Нукиев Б.А. Исследовательская деятельность в борьбе с незаконным оборотом наркотиков. Кокшетау: Кокшетауский государственный университет им. Ш. Уалиханова, 2017.

6. ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОММУНИКАЦИЙ И КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Тема 6.1. Особенности выявления и раскрытия преступлений в сфере коммуникаций и компьютерной информации

Значительное количество хищений сопряжено с предварительным посягательством на отношения, обеспечивающие безопасность соответствующих информационных ресурсов. В российском уголовном законодательстве данные деяния именуются как преступления в сфере компьютерной информации и определены в гл. 28 УК РФ.

Объектом данного преступления выступают общественные отношения, связанные с обеспечением конфиденциальности, целостности и (или) доступности охраняемой законом компьютерной информации.

Согласно ст. 16 ФЗ «Об информации» защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

По смыслу ст. 272 УК РФ к охраняемой законом информации следует относить не только информацию ограниченного доступа, но и общедоступную информацию, в отношении которой ее обладателем приняты меры по защите от несанкционированного уничтожения, модификации или блокирования.

Часть 3 ст. 272 УК РФ предусматривает три особо квалифицирующих признака неправомерного доступа к охраняемой законом компьютерной информации, совершенного группой лиц по предварительному сговору; организованной группой; лицом с использованием своего служебного положения.

Часть 4 ст. 272 УК РФ предусматривает два особо квалифицирующих признака: если такие действия повлекли тяжкие последствия или создали угрозу их наступления.

Объектом преступления выступают общественные отношения, связанные с обеспечением информационной безопасности от негативного воздействия вредоносной компьютерной информации и вредоносных компьютерных программ.

Содержание предмета данного преступления, а именно вредоносной компьютерной информации и вредоносной компьютерной программы, в целом выводится из грамматического, логического и формально-юридического анализа диспозиции ст. 273 УК РФ.

На правоприменительном уровне наиболее часто совершение данного преступления фиксируется при использовании и распространении вредоносных компьютерных программ, которые заведомо предназначены для генерации кода установки (серийного номера) и кода активации, запрашиваемых при установке лицензионных программных продуктов.

С объективной стороны преступление проявляется в совершении хотя бы одного из следующих действий:

- создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

- использование таких компьютерных программ или такой компьютерной информации;

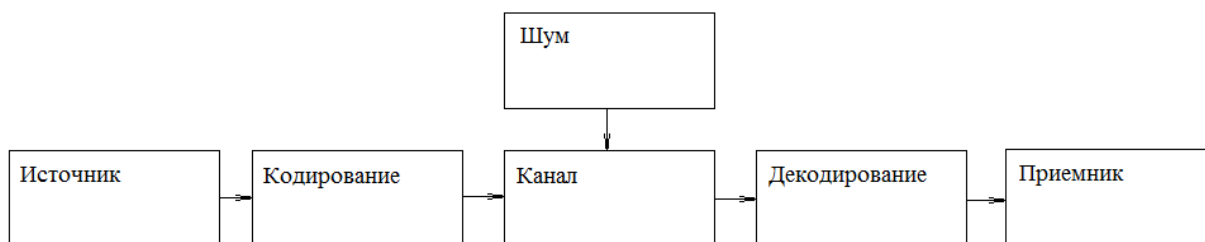
- распространение таких компьютерных программ или такой компьютерной информации.

Передача и хранение информации осуществляется с помощью различных знаков (символов), которые позволяют представить ее в некоторой форме.

Сообщение – совокупность знаков, отображающих некоторую информацию.

Сигнал – физический процесс, отображающий (несущий) передаваемое сообщение. В качестве сигналов в настоящее время в основном используются электрические и оптические сигналы. Сигнал передает (развертывает) сообщение во времени, т. е. всегда является функцией времени. Сигналы формируются путем изменения тех или иных параметров физического носителя в соответствии с передаваемым сообщением.

Модель системы передачи сигналов содержит: источник сигнала, блок кодирования, канал передачи информации, блок декодирования.



Под телекоммуникационными системами принято понимать структуры и средства, предназначенные для передачи больших объемов информации посредством специально проложенных линий связи или радиоэфира.

Телекоммуникационные системы различают:

по назначению:

- системы телевидения;
- системы связи (в том числе персонального вызова);
- компьютерные сети;

по типу используемой среды передачи информации:

- кабельные (традиционные медные);
- оптоволоконные;
- эфирные;
- спутниковые;

по способу передачи информации:

- аналоговые;
- цифровые.

Системы связи подразделяются по мобильности:

- на стационарные (традиционные абонентские линии);
- на подвижные.

Термин «вредоносное ПО» используется для описания любой вредоносной программы на компьютере или мобильном устройстве. Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера. Некоторые из наиболее распространенных типов вредоносных программ следующие.

1. Компьютерные вирусы, получившие свое название за способность заражать множество файлов на компьютере. Они распространяются и на другие СБТ при отправке зараженных файлов по электронной почте или их переносу пользователями на физических носителях, например на USB-накопителях.

2. Черви, в отличие от вирусов, распространяются без участия человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев.

3. Рекламное ПО, автоматически доставляющее рекламные объявления на хост-компьютеры и СВТ пользователей. Среди разновидностей: Adware – всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» ПО. Некоторые рекламные программы относительно безвредны, в других используются инструменты отслеживания для сбора информации о местонахождении пользователя, истории посещения им сайтов и вывода целевых объявлений (контента) на экран его СВТ.

4. Шпионское ПО следит за действиями пользователя на компьютере. Оно собирает информацию (например, регистрирует нажатия клавиш на клавиатуре компьютера, отслеживает посещение сайтов, перехватывает регистрационные данные), которая затем отправляется третьим лицам, как правило, киберпреступникам.

5. Программы-вымогатели заражают компьютер, затем шифруют отдельные файлы, например личные документы или фотографии, и требуют выкуп за их расшифровку. При отказе платить зашифрованные файлы удаляются.

6. Боты-программы, предназначенные для автоматического выполнения определенных операций. Проникнув в компьютер, боты могут заставить его выполнять определенные команды без ведома пользователя.

7. Руткиты позволяют третьей стороне получать удаленный доступ к компьютеру и управлять им. Эти программы используются IT-специалистами для дистанционного устранения сетевых проблем. Но в руках злоумышленников они превращаются в инструмент мошенничества.

8. Трояны – программы, которые маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в систему и осуществляют вредоносную деятельность без ведома жертвы.

9. Баги – ошибки в фрагментах программного кода. Они могут быть как допущены разработчиком ПО, так и появляться вследствие воздействия некоторых видов вредоносного ПО (например, вирусов, червей), и иметь пагубные последствия для СВТ, такие как остановка, сбой или снижение производительности.

Примерный план занятия

1. Виды преступлений, относящихся к категории «компьютерные преступления» и совершаемых в телекоммуникационных сетях.

2. Основные понятия и определения, используемые в ходе раскрытия преступлений, совершаемых в ИТКС. Сообщение и сигнал. Модель, системы передачи сигналов. Обобщенная модель системы передачи сигналов. Телекоммуникационная система. Особенности развития телекоммуникационных систем.

3. Уголовно-правовая и криминалистическая характеристика преступлений, совершаемых в сфере коммуникаций и компьютерной информации.

4. Вредоносные программы и компьютерные вирусы. Выявление и раскрытие преступлений, связанных с вредоносными компьютерными программами.

Вопросы для самоконтроля

1. В каком законе определено преступление в сфере компьютерной информации?

2. Что является объектом преступления в сфере компьютерной информации?

3. Что представляют собой мероприятия по защите информации?

4. Дайте определение понятиям «сообщение», «сигнал».

5. Из чего состоит модель системы передачи сигналов?

6. Дайте определение понятию «телекоммуникационная система», приведите примеры, классификацию.

7. Раскройте понятие «вредоносное ПО», перечислите некоторые типы «вредоносного ПО».

Тема 6.2. Выявление и раскрытие преступлений, совершаемых в системе дистанционного банковского обслуживания

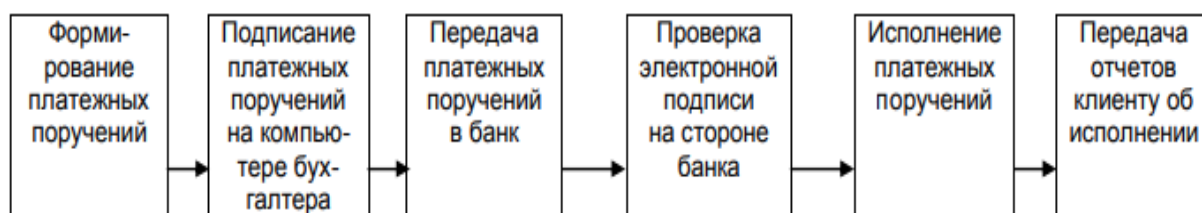
Дистанционное банковское обслуживание (ДБО) – это комплекс услуг удаленного доступа к различным банковским операциям, которые банки предоставляют своим клиентам.

Услуги ДБО – разноплановые электронные услуги, позволяющие обслуживать клиентов с использованием всех каналов доступа: Интернет (онлайн и офлайн доступ), телефон (обычный или мобильный), платежные терминалы и прочие.

Система ДБО – совокупность способов взаимодействия финансовой организации с клиентом.

<i>Системы дистанционного банковского обслуживания</i>		
Система «Клиент – банк»	«Телефон – банк»	Обслуживание через внешние устройства (банкоматы)
Взаимодействие строится через персональный компьютер, планшет или смартфон пользователя (переводы; оплата; открытие счетов и др.) <i>Этот тип подразделяется на два:</i> «Толстый клиент» – на ПК пользователя устанавливают специальную программу, она берет на себя основную нагрузку (принимает и обрабатывает данные), а удаленный сервер используется только для хранения данных. «Тонкий клиент» – все основные задачи по обработке информации переносятся на сервер.	Взаимодействие происходит через телефонную связь. Инструментом может выступать как мобильный, так и стационарный телефон. Можно отправить СМС-сообщения для разных операций. Например, запросить баланс, перевести средства или заплатить за мобильную связь, позвонить оператору и попросить его о какой-либо услуге. Допустим, нужно срочно заблокировать карту. Задавать команды через голосовое меню.	Распространенный способ получить банковские услуги без посещения отделений. Банкоматы часто бывают расположены по всему городу, даже в небольших населенных пунктах можно найти хотя бы один.

Схема работы ДБО



Нормативно-правовая база ДБО

1. Конституция Российской Федерации (принята всенародным голосованием 12121993)
2. Гражданский кодекс Российской Федерации (часть вторая) от 26011996 № 14-ФЗ
3. Федеральный закон от 27072006 № 152-ФЗ «О персональных данных»
4. Федеральный закон от 27062011 № 161-ФЗ «О национальной платежной системе»
5. Федеральный закон от 06042011 № 63-ФЗ «Об электронной подписи»
6. УПРФ от 17032008 г № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
7. Положение Банка России от 27 февраля 2017 года № 579-П «О Плانه счетов бухгалтерского учета для кредитных организаций и порядке его применения»
8. Положение Банка России от 29062021 № 762-П «О правилах осуществления перевода денежных средств»
9. Письмо Банка России от 07122007 № 197-Т «О рисках при дистанционном банковском обслуживании»

Способы совершения хищений денежных средств в системе ДБО

Ddos-атаки, подрыв репутации путем размещения в Интернете клеветы, оскорблений, а также мошенничество в системах дистанционного банковского обслуживания, взлом серверов и хищение конфиденциальной информации и денежных средств. Каждое из этих незаконных действий пагубно отражается на финансово-хозяйственной и иной деятельности пострадавших компаний и граждан. Но наибольший финансовый ущерб наносит мошенничество в системах интернет-банкинга.

Для отправки подложного платежного поручения мошенники могут использовать различные возможности вредоносных программ,

например отправить платежное поручение непосредственно с компьютера клиента банка с использованием средств удаленного управления или автоматически формировать мошенническое платежное поручение вирусом и подменять при помощи вредоносной программы реквизиты легитимного платежного поручения за мгновение до его подписания и передачи в банк. После отправки платежного поручения в банк основная задача преступников сводится к ограничению доступа легитимного пользователя к системе «Клиент – банк».

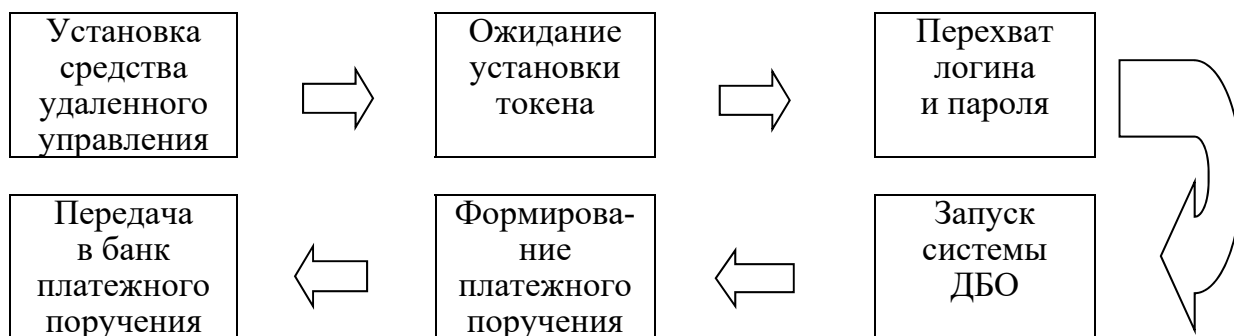
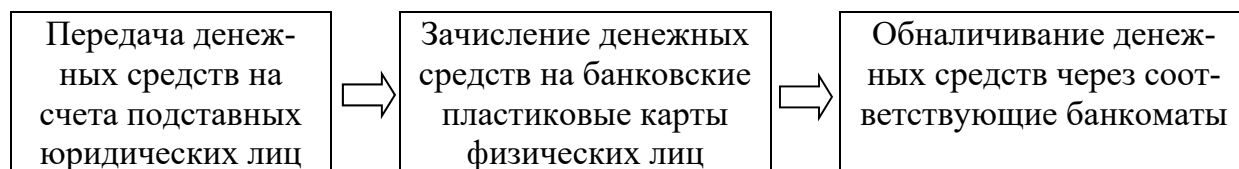


Схема обналичивания продумывается при подготовке к хищению денежных средств, предполагаемых к выведению. При небольших суммах часто используют банковские пластиковые карты физических лиц. Если же предполагается вывести значительные суммы денежных средств, преступники используют цепочку счетов подставных компаний и физических лиц с разделением средств на мелкие суммы для снятия денег через банкомат.



Приемы социальной инженерии

Помимо защиты от хищений при помощи технических устройств и уязвимости сетей, необходимо помнить, что мошенники очень широко применяют способ обманом заставить кого-то предоставить информацию или осуществить перевод денежных средств.

Виды атак при помощи социальной инженерии		
Претекстинг	Фишинг	«Охота» и фарминг
Использование предлога (например, опроса) для привлечения внимания жертвы и выяснения необходимых данных	Сообщения от кажущегося Вам надежным источника с целью выяснения необходимых данных	Долгосрочная связь с жертвой для выяснения большего объема данных

Действия сотрудников органов внутренних дел по раскрытию хищений денежных средств в системе ДБО

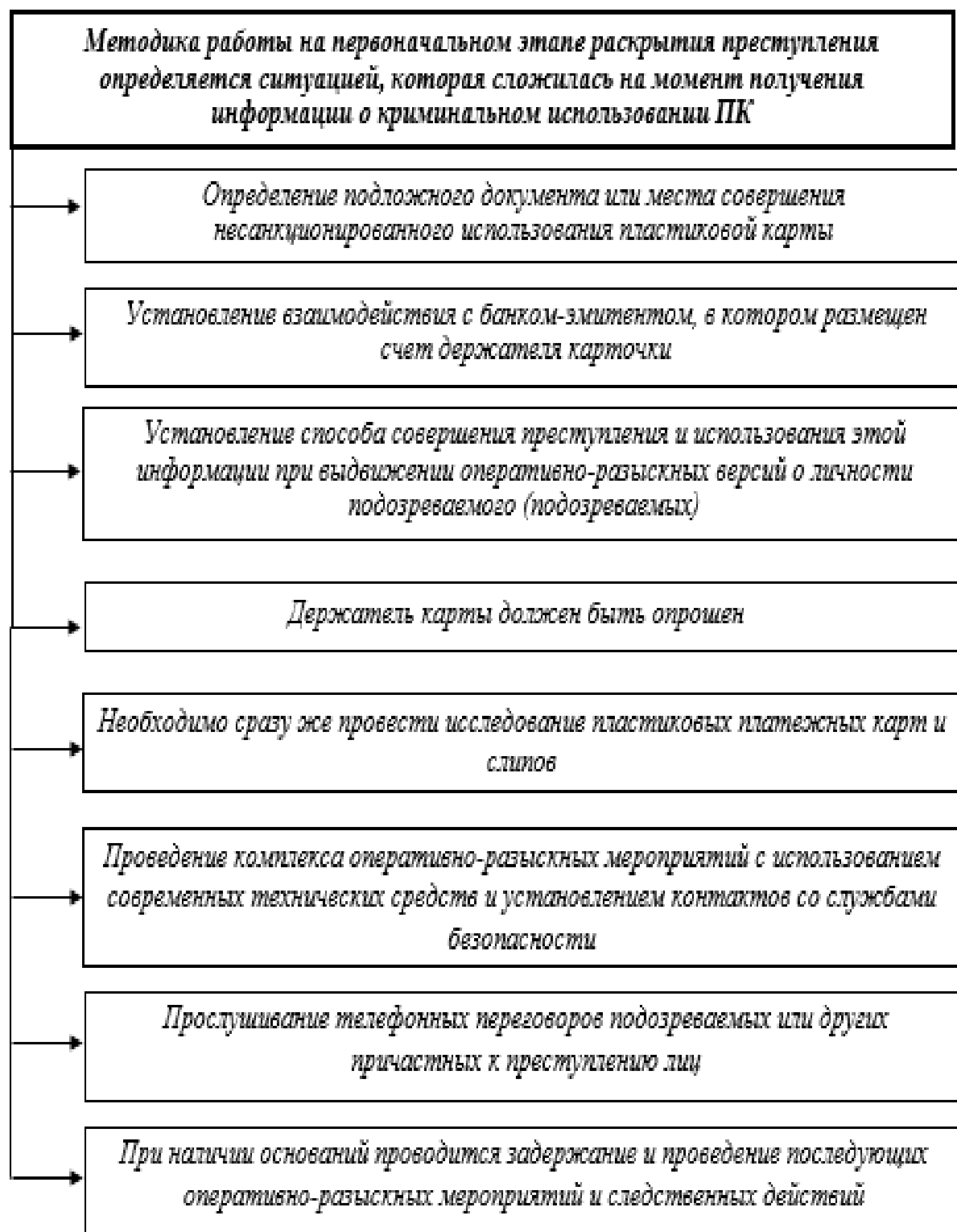
При выявлении хищений оперативные сотрудники должны ориентироваться на поиск лиц, обладающих специальными техническими познаниями в области ЭВМ. Установление лиц этой категории, выявление и пресечение их преступной деятельности возможны только на основе планомерного анализа оперативной обстановки, проведения как общих, так и ОРМ, а также изучения уголовной статистики.

В любой системе безналичных расчетов принимают участие три субъекта: *владелец карты – организация, выдавшая ее (эмитент); держатель карты и предприятие торговли (сервиса).*

Избранный преступником способ криминального использования пластиковых карт может стать опорной точкой при раскрытии для установления субъекта преступления. Выдвигая оперативно-разыскные версии о субъекте совершения преступлений с платежными пластиковыми картами, следует учитывать, что совершение преступлений с пластиковыми карточками (кроме их краж) требует специфических знаний в области их изготовления, технических требований к оформлению механизма их использования, знания иностранного языка, если карточка международная, и др.

Способы совершения преступлений могут быть классифицированы по четырем основным группам			
С использованием подлинных пластиковых карт	С фальсификацией (подлог и подделка) пластиковых карт и документов, сопровождающих их применение и незаконное использование	С использованием недействительных ПК	С использованием банкоматов

Данные преступления носят межрегиональный, международный характер, и расследование таких преступлений требует взаимодействия различных служб правоохранительных органов не только внутри страны, но и на международном уровне. Поэтому при борьбе с этим видом преступлений необходимо взаимодействие с правоохранительными системами других государств и использование возможностей Интерпола.



Вопросы сотрудника ОВД в ходе выявления и раскрытия преступлений, совершаемых сотрудниками банков		
<i>Общие вопросы</i>	<i>Характеристика системы защиты информации</i>	<i>Персонализирующие признаки персонала</i>
1. Существует ли в данном кредитно-финансовом учреждении локальная сеть для осуществления кредитно-денежных операций? 2. Существуют ли в кредитно-финансовом учреждении специальная служба по эксплуатации локальной компьютерной сети и служба безопасности, ответственные за ее функционирование? Каков состав и обязанности их сотрудников? 3. Как осуществляется доступ в помещения, оснащенные компьютерной техникой, при помощи которой производятся финансовые расчеты?	1. Сертифицированы ли программы системной защиты? 2. Используются ли проблемно-ориентированные технические средства защиты финансовой информации? Имеются ли пароли защиты и как часто происходит их смена? 3. Установлены ли идентификационные программы? Имеются ли в рабочих программах специальные файлы протоколов, регистрирующие вхождение в систему пользователей, и каково их содержание?	1. Кто выполняет обязанности системного администратора сети? Как и в каком порядке им осуществляется системное администрирование? 2. Кто из работников учреждения допущен к работе с финансовыми компьютерными программами и кто из них обладает правами на внесение изменений в эти программы, каков объем их прав? 3. Кто из работников кредитно-финансового учреждения в течение интересующего периода времени был уволен и по каким мотивам?

Способы установления лица, причастного к хищению, с использованием сети Интернет

Соединение между компьютерами в сети Интернет происходит по протоколу TCP/IP. Каждый компьютер в сети TCP/IP имеет **адреса трех уровней**:

OSI	TCP/IP	Протоколы	
7. Прикладной	5. Прикладной	DNS, HTTP (WWW), FTP, SMTP, TFTP, NFS,...	
6. Представления			
5. Сеансовый			
4. Транспортный	4. Транспортный	TCP	UDP
3. Сетевой	3. Сетевой	ARP, RARP	ICMP
		IGMP	RIP, OSPF, BGP
2. Канальный	2. Звена данных	Протоколы определяются технологией сети	
1. Физический	1. Физический		

Зная **IP-адрес** компьютера, возможно установить личность владельца компьютера, обратившись с запросом к провайдеру, у которого данный IP зарегистрирован.

При передаче файла от одного компьютера к другому возникает соединение между двумя компьютерами, и пока идет передача файла, можно установить IP.

Онлайн «сниффер», или *http web sniffer (eng)*, – это специальная программа на PHP, откладывающая в специальный файл на сервере информацию о пользователе, а именно: его IP-адрес, время посещения страницы-сниффера, а также адрес страницы, с которой пользователь сделал переход на «сниффер».

Если сайт является форумом, на котором происходит регистрация пользователей, получив доступ с административными правами к данному ресурсу, можно получить полную базу пользователей с IP-адресами, и, в случае выявления среди них нарушителей закона, привлечь их к уголовной ответственности.

Источники получения информации сотрудниками ОВД для раскрытия преступлений в сфере ДБО



Профилактика хищений денежных средств в системе ДБО

В целях недопущения хищений денежных средств необходимо следующее.

1. *Повышать уровень цифровой и финансовой грамотности.*
2. *Использовать надежные современные СВТ.* В случае неожиданного выхода из строя компьютера во время работы с системой «Клиент – банк» немедленно отключить от компьютера средства аутентификации (например, USB-ключ).
3. *При внезапном прекращении работы сим-карты мобильного устройства необходимо обратиться к оператору сотовой связи за уточнением причин.*
4. *Использовать компьютер исключительно для обеспечения работы в системе «Клиент – банк». Не устанавливать на этом компьютере ПО без особой необходимости.* Не запускать неизвестные программы, не открывать почтовые вложения. Не использовать компьютер для игр и интернет-серфинга. В случае необходимости работы в Интернете использовать только проверенные сайты по заранее определенному списку адресов.
5. *Использовать лицензионную операционную систему Windows, лицензионное антивирусное ПО.*
6. *Использовать надежные пароли.*

7. Не отвечать на подозрительные письма с просьбой выслать секретный ключ ЭП, пароль и другие конфиденциальные данные. Банк никогда не осуществляет рассылку электронных писем с компьютерными программами или с просьбой предоставить конфиденциальную информацию.

8. Регулярно контролировать состояние своих счетов и незамедлительно информировать обслуживающее подразделение Банка обо всех подозрительных или несанкционированных операциях. В случаях подозрений на мошеннические действия в системе ДБО, незамедлительно обращаться в правоохранительные органы.

Примерный план семинара

1. Система дистанционного банковского обслуживания.
2. Способы совершения преступлений в системе дистанционного банковского обслуживания.
3. Особенности выявления и предупреждения преступлений в системе дистанционного банковского обслуживания.

Вопросы для самоконтроля по теме

1. Поясните содержание понятий «дистанционное банковское обслуживание» и «услуги дистанционного банковского обслуживания».
2. Какие элементы входят в систему дистанционного банковского обслуживания? Дайте характеристику каждому из элементов.
3. Опишите схему обналичивания подложного платежного поручения.
4. Что понимается под социальной инженерией?
5. Какие виды атак при помощи социальной инженерии используют мошенники?
6. Каковы особенности выявления и предупреждения преступлений в системе дистанционного банковского обслуживания?
7. Какую информацию должен выяснить сотрудник ОВД в ходе выявления и раскрытия преступлений, совершаемых сотрудниками банков?
8. Какие ОРМ необходимо провести при установлении факта перечисления денежных средств?
9. Из каких источников сотрудники ОВД могут получить информацию для раскрытия преступлений в сфере ДБО?
10. Что необходимо предпринять для недопущения хищений денежных средств?

Тема 6.3. Выявление фактов вовлечения несовершеннолетних в деструктивную деятельность посредством информационно-коммуникационных технологий

Деструктивное поведение несовершеннолетнего – это разрушительное поведение, направленное вовне или на самого себя, приводящее к нарушению качества жизни человека, снижению критичности к своему поведению, когнитивным искажениям восприятия и понимания происходящего, эмоциональным нарушениям, что в итоге приводит к состоянию социальной дезадаптации личности. Основными опасностями деструктивного поведения являются: насилие, убийства, самоубийства, наркомания, алкоголизм, радикализм, сатанизм и т. п. Нагляднее всего деструктивное поведение проявляется в подростковом возрасте, когда особенности психики в совокупности с проблемой социализации и недостатком внимания со стороны взрослых могут привести к деструктивным изменениям личности и формированию преступного поведения несовершеннолетнего.

При современном состоянии развития и распространения социального медиа наиболее «оптимальным» инструментом для вовлечения несовершеннолетних в деструктивную деятельность являются ИКТ, посредством которых происходит социальное научение и закрепление у несовершеннолетних нормальности и приемлемости девиантного (делинквентного) поведения (сцены агрессии, насилия и жестокости, наполняющие эти сферы, глубоко укореняются у несовершеннолетнего, начинают восприниматься им как должное, а со временем занимают приоритетное место в иерархии его интересов).

Основные цели вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ:

- массовое распространение деструктивной информации в социальных медиа посредством ИКТ;
- обесценивание традиционных ценностей; формирование у подростков искаженных ценностей;
- создание у пользователей социальных медиа ощущения неблагополучия и опасности не только в сетях – в виртуальном мире, но и в государстве – в объективной реальности;
- вербовка внушаемых и ориентированных на деструктив людей для дальнейшего вывода их деструктивной активности в объективную реальность;
- дестабилизация социальной и политической жизни государства.

Под воздействием деструктивного влияния у несовершеннолетних, вовлеченных в деструктивные течения, образуются устойчивые поведенческие паттерны разрушительного типа.

1. Снижение способности самостоятельно думать и принимать решения. Отсутствие желания учиться, развиваться, работать. Желание деградировать и быть лучшим из худших.

2. Отрицание всякой ответственности. Поиск внешней идеологии, четкого алгоритма действий как стремление передать ответственность за свою жизнь другому.

3. Отсутствие авторитетов среди значимых взрослых. Восприятие родителей, учителей, знакомых как людей отсталых, глупых, ниже себя по уровню развития.

4. Обесценивание норм морали и общечеловеческих ценностей. Стремление нарушать правила, бороться и уничтожать. Такое поведение в принципе свойственно подростковому возрасту, в данном случае речь идет именно о радикальных проявлениях.

5. Выраженная симпатия подростков к антигероям, антидвижениям и всему, что можно назвать темной стороной (зло). Все злое воспринимается как насыщенная и яркая жизнь, все нормальное – как скучное и тяжелое.

6. Выраженное стремление подростков к разрушению на всех уровнях: своей психики, своего тела, своего окружения, вещей, идей, государства, общества, культуры, морали и т. п. Подростки хотят разрушать и быть разрушенными.

Основные виды деструктивной деятельности несовершеннолетних посредством ИКТ

1. Вовлечение несовершеннолетних в распространение идей экстремизма и терроризма	Вовлечение несовершеннолетних в ультра движения политического характера (анархические, неонацистские и т. д.)
	Вовлечение несовершеннолетних в криминальные субкультуры (АУЕ, агрессивные футбольные фанаты и т. д.)
	Вовлечение несовершеннолетних в группы шок-контента (группы массовых убийств, течения колумбайн, скулшутинга)

2. Вовлечение несовершеннолетних в аутидеструктивное поведение	Вовлечение несовершеннолетних в «группы смерти», суицидального призыва, призывы к членовредительству
	Вовлечение в группы, пропагандирующие рискованное поведение: зацепинг (езда между или под вагонами, на хвостовом вагоне или на крыше); руфинг (передвижение по высотным точкам зданий); диггерство (непрофессиональное исследование искусственных подземных сооружений); инфильтрация (проникновение на охраняемые территории); опасные селфи и т. д.
3. Вовлечение несовершеннолетних в аддиктивное (зависимое) поведение	Формирование у несовершеннолетней химической зависимости (алкоголизм, наркомания, токсикомания) с их дальнейшим рекрутированием для распространения и продажи запрещенных веществ и наркотических средств
	Формирование игровой зависимости (компьютерная зависимость и зависимость к азартным играм)
	Нарушение пищевого поведения несовершеннолетнего (анорексия, булимия, переедание)
4. Деяния против половой неприкосновенности, совершаемые несовершеннолетними или по отношению к ним	Доступ к личным материалам интимного характера (фотографиям, видеоизображениям) несовершеннолетнего и дальнейшая их отправка или опубликование («секстинг»)
	Домогательство и (или) совершение сексуальных действий в онлайн-пространстве (онлайн-груминг, виртуально-сексуальное насилие)

Наиболее распространенное понимание сущности вовлечения несовершеннолетнего в деструктивную деятельность означает создание решимости или готовности участвовать в совершении общественно опасных противоправных действий, направленных на реализацию преступного умысла. Вовлечение предполагает активные действия взрослых, связанные с физическим и психологическим воздействием на несовершеннолетнего. Вовлечение выражается во внушении несовершеннолетнему мысли о необходимости совершения деструктивного действия. Типовая схема вовлечения несовершеннолетних в противоправную деятельность выглядит следующим образом: подбор несовершеннолетнего; формирование в качестве приемлемой модели антиобщественного поведения и противоправных установок;

укрепление желания совершить конкретное преступление или антиобщественное действие; сокрытие участия взрослого в совершении преступления или антиобщественного действия.

■ **Формы вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ:**

1) чаты и форумы в социальных сетях (Twitter, Instagram, TikTok, «ВКонтакте», «Мой мир», Facebook);

2) распространение деструктивного контента;

3) геймификация («игровизация»): игры квазинейтральные («Пропасть на 72/24 часа», «Ночь в заброшенной гостинице», «24 часа в чужой квартире» и др.); игры, опасные для жизни и здоровья («Перебеги на красный», «Беги или умри», «Подожги себя» (FIRE-challenge), «Прокатись на крыше авто» и др.); видеоигры, пропагандирующие насилие (стрелялки и т. д.); суицидальные игры-квесты;

4) создание и распространение мемов деструктивного характера (мемы-оскорбления ветеранов и видеоигры, искажающие историю Второй мировой войны и т. д.);

5) призывы участия во флешмобах.

Вовлечение несовершеннолетних в деструктивную деятельность, в том числе в деятельность запрещенных в Российской Федерации движений, обусловлено комплексом факторов и причин. Часто невозможно выделить какой-либо один или группу маркеров (критериев), наличие которых однозначно свидетельствовало бы о вовлечении несовершеннолетних в ту или иную деструктивную деятельность. Вовлечение в деструктивную деятельность посредством ИТК может характеризоваться различным набором действий, например эпизодическое чтение и репост соответствующих текстов экстремистской тематики с одной стороны и непосредственное участие в совершении преступления с другой. Следовательно, определение степени вовлеченности несовершеннолетнего носит индивидуальный характер.

■ **Критерии (маркеры) вовлечения несовершеннолетнего в деструктивную деятельность на основе анализа его профиля в Интернете.**

1. Оценка частоты посещения несовершеннолетним интернет-сайтов (страниц, форумов и т. д.) деструктивного характера и время, проводимое в них.

1.1. Интерес несовершеннолетнего к сайтам (группам, форумам, сообществам) с шок-контентом в сети Интернет.

1.2. Интерес несовершеннолетнего к расовой теории, которая основывается на постулате о том, что человеческие расы различаются и высшие расы имеют превосходство над низшими.

1.3. Интерес и оправдание культа жестокости и насилия, выраженные среди прочего в поисках и сохранении фото- и видеоматериалов неспортивного насилия.

1.4. Интерес несовершеннолетнего к культуре употребления наркотических веществ, к высказываниям известных людей о собственном положительном опыте употребления запрещенных веществ.

1.5. Интерес к самоубийствам и их романтизация.

2. Анализ влияния содержания контента аккаунтов в социальных сетях, принадлежащих несовершеннолетнему, на степень принятия деструктивного поведения и (или) принадлежность к определенному маргинальному сообществу. Анализу подвергаются текстовые, фото- и видеоматериалы.

3. Анализ содержания комментариев несовершеннолетних в социальных сетях как показатель положения деструктивной деятельности в системе его собственных ценностей.

4. Определение круга общения несовершеннолетнего (друзья, подписчики) и выявление в нем лиц с выраженной деструктивной направленностью, а также определение отношения несовершеннолетнего к этим лицам через реакцию одобрения, позитивные высказывания в их адрес.

5. В компьютерных (сетевых) играх, в которых присутствуют сцены насилия, через игровые инструменты поощряется совершение противоправных действий.

6. Интерес к биографии криминальных авторитетов и иных профессиональных преступников, популяризация и оправдание их преступной деятельности посредством размещения сообщений и комментариев в сети Интернет.

7. Хранение на персональном компьютере, смартфоне и иных гаджетах, а также цифровых носителях материалов о криминальной субкультуре, противоправных деяниях, в том числе фото-, видеоматериалов, текстов, картинок и т. д.

8. Наличие факта перечисления денежных средств на так называемый «общак», т. е. финансирование неформальных организаций, материальная поддержка лиц, находящихся в следственном изоляторе и местах лишения свободы, перевод денежных средств на поддержание сообществ и групп, аккаунтов в социальных сетях и мессенджеров.

9. Несформированность у несовершеннолетних позитивных интересов.

10. Наличие у несовершеннолетнего закрытого круга общения в сети Интернет (участие в закрытых форумах, группах и т. д.).

Алгоритм вовлечения несовершеннолетнего несовершеннолетних в деструктивную деятельность посредством ИКТ:

Шаг № 1 «Зацепка»	Установление контакта с несовершеннолетним, провокация диалога через: совместную игровую деятельность (онлайн игры); одобрение самовыражения (лайки, репосты в социальных сетях); коммерческие предложения «невинного толка» для легкого заработка; формирование импульса к любопытству
Шаг № 2 «Аффилиация»	Формирование у несовершеннолетнего заинтересованного равнодушного отношения к актору (вербовщику), вступившему с ним в контакт
Шаг № 3 «Оценка»	Выявление у несовершеннолетнего индивидуальных «болевых точек» (проблемы с родителями, сверстниками, конкретные конфликты, комплексы и т. д.)
Шаг № 4 «Воздействие»	Индивидуальное информационное воздействие, вовлечение в диалог на конкретную деструктивную тематику (экстремизм, терроризм, суицид, наркотики и т. д.)
Шаг № 5 «Эмоции»	Формирование у несовершеннолетнего желаемого образа отношений к конкретной деструктивной деятельности
Шаг № 6 «Поведение»	Формирование у несовершеннолетней готовности к деструктивной деятельности и к конкретному деструктивному действию

В процессе вовлечения используются несколько постулатов, влияющих на сознание несовершеннолетних: «Деструктив (колумбайн, анархизм, суицид, наркотики и пр.) делает тебя особенным. Ты отличаешься от серой массы. Твоя жизнь становится ярче»; «Быть жестоким и совершать преступления – весело и классно»; «Насилие – отличный способ избавиться от напряжения»; «Быть убийцей и террористом – круто»; «Пора что-то делать в реальной жизни» и т. д.

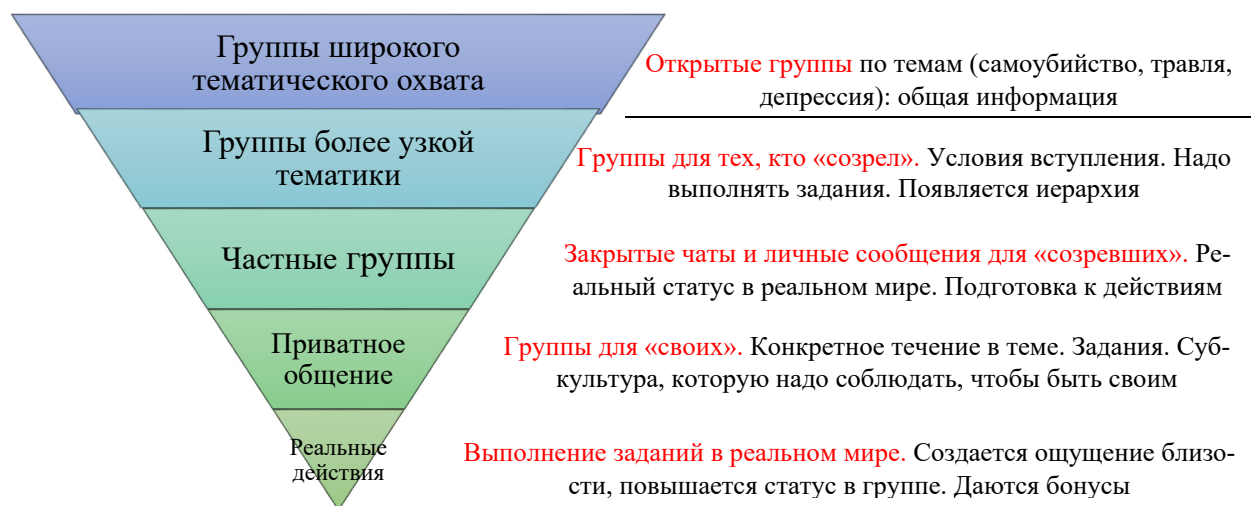
Готовность несовершеннолетнего к совершению деструктивных действий оценивается по следующим уровням.

1 уровень – размышление о возможности. На уровне размышлений о возможности совершения деструктивного деяния поведенческие признаки участия в деструктивном течении единичны, несовершеннолетний говорит о том, что возможно он когда-нибудь попробовал такое или размышляет о возможности того, что подобный инцидент может произойти поблизости.

2 уровень – формирование желания. Поведенческие признаки более выражены, несовершеннолетний говорит, что сам хочет сделать так; хочет попробовать; сделает, как только будет возможность.

3 уровень – планирование, затем совершение. Присутствуют многие поведенческие признаки: подросток сообщает об инциденте, в будущем совершенном «когда я вас расстреляю», «вот когда я буду закладывать наркотики», или сообщает о подготовке к инциденту напрямую.

Эффективность вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ определяется тем, что в интернет-пространстве легко происходит замыкание внимания пользователя на определенном типе информации или волнующих его проблемах и отгораживание от альтернативной информации, не укладывающейся в систему его взглядов. В этом случае получаемая информация будет только подтверждать и укреплять уже имеющиеся взгляды пользователя, возможность столкнуться с альтернативными точками зрения существенно снижена. Вовлечение несовершеннолетних в деструктивную деятельность вне зависимости от характеристики самой деятельности происходит посредством вовлечения несовершеннолетнего в виртуальные сообщества. Деструктивные группы в сети Интернет устроены таким образом, что на поверхности самой группы нет ничего запрещенного, это могут быть картинки, различные опросы, простые записи, видео, несущие обычную информацию без каких-либо элементов вовлечения. После этого организаторы, видя, что именно заинтересовало того или другого участника группы, вовлекают его уже в дальнейшие действия: это может быть переписка в закрытых чатах либо другие действия в офлайн-режиме.



Процедуры нейтрализации деструктивных намерений несовершеннолетнего на разных уровнях (этапах) готовности к действию:

1. На этапе размышления о возможности необходимо разъяснять несовершеннолетнему негативные последствия такого поведения, аккуратно переключать его внимание на другую сферу.

2. На этапе формирования желания необходимо разъяснить негативные последствия такого поведения, а затем, используя имеющиеся ресурсы, приступить к решению проблем несовершеннолетнего, оказывать ему сопровождение.

3. На этапе планирования необходимо сказать о негативных последствиях такого поведения, а затем, используя ресурсы, помочь в решении проблем несовершеннолетнего и поставить его на учет психолога для коррекционной работы.

Меры противодействия технологиям вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ

Направления деятельности	Цель и способы достижения
Профилактическая работа с несовершеннолетними, находящимися в группе риска, потенциально способными присоединиться к деструктивным молодежным движениям	Выработка определенного сценария поведения, при котором несовершеннолетний будет осуществлять себя значимым как для общества в целом, так и для отдельных индивидуумов
Осуществление обмена информации между субъектами профилактики	Сотруднику полиции необходимо постоянно поддерживать контакт с представителями образовательных учреждений (педагогик, психологи)

Профилактическая работа с законными представителями несовершеннолетних	Необходимо разъяснять признаки вовлечения несовершеннолетних в деструктивную деятельность, способы вовлечения, указывать на необходимость контроля круга общения своего ребенка как в реально жизни, так и в социальных сетях
Мониторинг сети Интернет	Мониторинг ресурсов проводится на предмет выявления деструктивных интернет-сообществ, которые осуществляют вовлечение несовершеннолетних в свою противоправную деятельность

Деятельность подразделений Министерства внутренних дел РФ в сфере профилактики вовлечения несовершеннолетних в деструктивные группы ведется на постоянной основе. В целях профилактики правонарушений в молодежной среде, в частности, выявления деструктивных и суицидальных групп несовершеннолетних, сотрудники территориальных органов МВД России проводят мониторинг сети Интернет. Их деятельность направлена на выявление сайтов администраторов и кураторов так называемых «групп смерти», а также страниц в сети Интернет, пропагандирующих суициды и вовлекающих несовершеннолетних в совершение действий, причиняющих вред здоровью.

В рамках информационно-просветительской работы в образовательных организациях на родительских собраниях разъясняются особенности поведения подростков, причисляющих себя к «колумбайнерам», «скинхедам», футбольным фанатам, вступления детей в «группы смерти» и признаки суицидальных проявлений.

Министерство внутренних дел РФ организует и проводит комплекс мероприятий информационно-пропагандистской направленности с вовлечением несовершеннолетних, состоящих в военно-патриотических клубах

В целях противодействия вовлечению несовершеннолетних в деструктивные группы в сети Интернет на территории Российской Федерации осуществляет свою деятельность рабочая группа, созданная распоряжением МВД России от 21.03.2017 № 1/3236 из числа представителей служб и подразделений МВД России, заинтересованных в выработке и реализации неотложных мер, направленных на совершенствование механизма выявления, предупреждения, пресечения и раскрытия преступлений, связанных с деятельностью лиц, склоня-

ющих несовершеннолетних к деструктивному поведению посредством оказания психологического воздействия через Интернет .

Примерный план семинара

1. Асоциальное поведение несовершеннолетнего в сфере ИКТ.
2. Аутдеструктивное поведение несовершеннолетнего в сфере ИКТ.
3. Аддиктивное поведение несовершеннолетнего в сфере ИКТ.
4. Способы и механизм вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ.
5. Меры противодействия технологиям вовлечения несовершеннолетних в деструктивную деятельность посредством ИКТ.

Вопросы для самоконтроля по теме

1. Перечислите маркеры (признаки) несовершеннолетних, вовлекаемых в деструктивную деятельность посредством ИКТ.
2. Дайте определения и приведите примеры нежелательного контента, его виды и воздействия на интеллектуальное, эмоциональное, психическое здоровье личности.
3. Опишите особенности профилактики деструктивного поведения в сфере ИКТ среди несовершеннолетних.

Тема 6.4. Использование биометрических технологий и методов, способствующих раскрытию преступлений

В соответствии с приказом №70 от 10.02.2006 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации» экспертно-криминалистическим учетом является система хранения и поиска экспертно-криминалистической информации об объектах учета, используемая для решения задач оперативно-розыскной деятельности и расследования уголовных дел. Экспертно-криминалистическая информация представляет собой индивидуальную совокупность криминалистически значимых признаков объекта учета, выявляемых и фиксируемых с использованием специальных знаний, экспертно-криминалистических методов и средств.

Экспертно-криминалистические учеты органов внутренних дел ведутся:

- в федеральном государственном казенном учреждении «Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации», – федеральные учеты;

- в экспертно-криминалистических центрах министерств внутренних дел по республикам, главных управлений, управлений Министерства внутренних дел РФ по иным субъектам Российской Федерации по преступлениям, совершенным на территории соответствующего субъекта Российской Федерации, включая территории обслуживания управлений на транспорте МВД России по федеральным округам, Восточно-Сибирского и Забайкальского линейных управлений внутренних дел на транспорте МВД России, либо на территории нескольких субъектов Российской Федерации, определяемых МВД России, – региональные учеты;

- в структурных подразделениях ЭКЦ по экспертно-криминалистическому обеспечению управлений, отделов, отделений Министерства внутренних дел Российской Федерации по районам, городам и иным муниципальным образованиям, в том числе по нескольким муниципальным образованиям, управлений, отделов, отделений Министерства внутренних дел РФ на части территорий административных центров субъектов РФ, управлений, отделов, отделений Министерства внутренних дел РФ по закрытым административно-территориальным образованиям, на особо важных и режимных объектах, линейных отделах, отделениях Министерства внутренних дел РФ на железнодорожном, водном и воздушном транспорте, в экспертно-

криминалистических подразделениях территориальных органов МВД России на районном уровне, – районные учеты.

Ведение экспертно-криминалистических учетов осуществляется сотрудниками ЭКП и представляет собой деятельность по систематизации и размещению в информационной системе экспертно-криминалистической информации об объектах учета, позволяющей осуществить ее использование в целях решения задач оперативно-розыскной деятельности и расследования уголовных дел.

Основной формой ведения экспертно-криминалистических учетов является картотека, состоящая из информационных карт установленной формы, содержащих закрепленную и систематизированную индивидуальную экспертно-криминалистическую информацию об объектах учета.

Перечень экспертно-криминалистических учетов органов внутренних дел Российской Федерации

Код учета	Наименование учета	Целевое назначение	Объекты учета	Формы и уровни ведения учета
01	Учет следов рук	Установление лиц, оставивших следы рук на месте происшествия, фактов оставления следов рук одним и тем же лицом при совершении нескольких преступлений	Следы рук, изъятые с мест преступлений	Информационные карты (форма ИК-1) с фотоснимками следов рук в масштабах 1:1, 2:1 или 3:1. Федеральный, региональный, районный
02	Учет следов подошв обуви	Установление лиц, оставивших следы обуви на месте происшествия, фактов оснащения следов одного и того же экземпляра обуви при совершении нескольких преступлений	Следы подошвы обуви, изъятые с мест преступлений	Информационные карты (форма ИК-1) с фотоснимками следов обуви в масштабе 1:1 или 1:2 (для оставленных всей подошвой). Региональный, районный
03	Учет следов орудий взлома	Установление орудий взлома, оставивших следы на месте происшествия, фактов использования одного и того же орудия взлома при совершении нескольких преступлений	Следы отжима, иные трасологические следы с достаточной степенью отображения индивидуальных особенностей следообразующих инструментов, изъятые с мест преступления	Информационные карты (форма ИК-1) с фотоснимками следов орудий взлома в масштабе 3:1. Региональный, районный

04	Учет следов протекторов шин транспортных средств	Установление авто-транспортных средств, оставивших следы на месте происшествия, фактов использования одного и того же автотранспортного средства при совершении нескольких преступлений	Следы протекторов шин транспортных средств, изъятые с мест преступлений и происшествий	Информационные карты (форма ИК-1) с фотоснимками следов протекторов шин в масштабе от 1:4 до 1:2. Региональный, районный
05	Строка утратила силу – приказ МВД России от 28.12.2016 № 918.			
06	Учет микрообъектов (микроволокон, частиц лакокрасочных покрытий, полимеров и металла)	Установление однородности происхождения микрообъектов, обнаруженных на местах происшествий или (и) изъятых в качестве образцов у подозреваемых в совершении преступлений лиц	Микрообъекты (микроволокон, частицы лакокрасочных покрытий и металла), изъятые с мест преступлений	Информационные карты (форма ИК-9) с фотоснимками, спектрограммами, иными сведениями о строении, составе и локализации микрообъектов, натурные объекты. Региональный (по тяжким и особо тяжким преступлениям)
07	Учет самодельных взрывных устройств	Установление единого источника происхождения самодельных взрывных устройств (их основных элементов и механизмов) по конструктивным и технологическим особенностям изготовления	Самодельные взрывные устройства (СВУ), их основные элементы и остатки после взрыва	Информационные карты (форма ИК-3), фототаблицы и схемы со сведениями о СВУ; натурные объекты, не содержащие радиоэлектронику (на региональном уровне) и содержащие радиоэлектронику (на федеральном уровне), не включающие в себя взрывчатых веществ и взрывоопасных элементов. Федеральный, региональный
08	Учет самодельного огнестрельного оружия	Установление единого источника происхождения самодельного огнестрельного оружия (его отдельных частей, механизмов) по конструктивным и технологическим особенностям его изготовления	Самодельное или переделанное огнестрельное оружие, предусмотренное п. 35 Правил ведения экспертно-криминалистических учетов	Информационные карты (форма ИК-4) с фотоснимками, натурные объекты. Федеральный (картотека), региональный

09	Учет пуль, гильз и патронов со следами ручного стрелкового огнестрельного оружия, изъятых с мест происшествий и преступлений	Установление конкретного экземпляра, фактов применения одного и того же экземпляра оружия при совершении нескольких преступлений	Пули, гильзы и патроны (калибра не более 14,5 мм) со следами нарезного огнестрельного оружия, изъятые с мест происшествий	Информационные карты (форма ИК-10), натурные объекты, электронная база данных. Федеральный, региональный
10	Учет контрольных пуль и гильз утраченного служебного, гражданского, боевого огнестрельного оружия с нарезным стволом, боевого ручного стрелкового оружия	Установление фактов использования утраченного служебного, гражданского, боевого огнестрельного оружия при совершении преступлений	Контрольные пули и гильзы утраченного нарезного служебного, гражданского, боевого огнестрельного оружия калибра не более 14,5 мм	Натурные объекты, электронная база данных. Федеральный
11	Учет поддельных денежных билетов, бланков ценных бумаг и бланков документов	Установление единого способа изготовления выявленных поддельных денежных билетов Банка России, иностранной валюты, бланков ценных бумаг и бланков документов	Полностью поддельные и частично измененные денежные билеты Банка России и в иностранной валюте, бланки ценных бумаг. Поддельные бланки документов федерального и регионального значения	Информационный массив, натурные объекты. Федеральный, региональный
12	Учет поддельных монет	Установление единого источника происхождения выявленных поддельных монет	Поддельные металлические деньги (монеты) Банка России и в иностранной валюте	Информационные карты (форма ИК-11) с фотоснимками аверса, реверса монет в масштабе 5:1, натурные объекты. Федеральный
13	Учет субъективных портретов разыскиваемых лиц	Установление личности разыскиваемых лиц по описанию их внешности	Субъективные портреты разыскиваемых лиц	Информационные карты (форма ИК-6) с субъективными портретами лиц в масштабе с межзрачковым расстоянием 20 мм. Региональный, районный
14	Строка утратила силу с 01.11.2018 – приказ МВД России от 11.09.2018 № 585.			

15	Краниологический учет (учет черепов неопознанных трупов)	Установление личности по черепам неопознанных трупов	Череп неопознанных трупов, фрагменты костей черепа, зубные протезы, мосты, коронки, представленные на исследование вместе с черепом	Информационные карты (форма ИК-8), натурные объекты. Региональный
16	Строка дополнительно включена приказом МВД России от 28.12.2016 № 918; утратила силу с 01.11.2018 – приказ МВД России от 11.09.2018 № 585.			
17	Строка дополнительно включена приказом МВД России от 28.12.2016 № 918; утратила силу с 01.11.2018 – приказ МВД России от 11.09.2018 № 585.			

Учет следов рук

Учет следов рук предназначен для установления лиц, оставивших следы рук на месте происшествия, а также фактов принадлежности следов рук, изъятых по нескольким преступлениям, одному и тому же неустановленному лицу. Данный учет ведется на федеральном, региональном и районном уровнях.

Допускается формирование и ведение учета в виде электронных баз данных. При этом автоматизированный режим ведения учета осуществляется с использованием централизованной интегрированной автоматизированной дактилоскопической информационной системы Министерства внутренних дел Российской Федерации (ЦИАДИС-МВД) в порядке, установленном нормативными правовыми актами МВД России.

Ведение автоматизированного учета следов рук осуществляется в соответствии с эксплуатационной документацией ЦИАДИС-МВД сотрудниками, прошедшими соответствующую подготовку. При этом к работе по проверке рекомендательных списков допускаются только эксперты, аттестованные на право самостоятельного производства дактилоскопических экспертиз.

Картотека учета формируется из информационных карт установленного образца «Форма ИК-1», на обратной стороне которых размещаются фотоснимки следов рук неустановленных лиц в масштабах 1:1, 2:1 или 3:1, признанных пригодными для идентификации и выполненных по правилам детальной съемки (наличие масштабной линейки в основании следа).

Информационные карты составляются в двух экземплярах и регистрируются в журнале регистрации объектов, поступивших на экспертно-криминалистический учет (приложение № 1 к Инструкции по организации использования экспертно-криминалистических учетов

органов внутренних дел). Один экземпляр помещается в дактилоскопическую следотеку ЭКП территориального органа МВД России на районном уровне, второй экземпляр не реже трех раз в месяц направляется в территориальный орган МВД России на региональном уровне.

В случае получения отрицательного результата проверки следов рук, изъятых с мест преступлений, по региональному учету территориальный орган МВД России на региональном уровне направляет электронные копии следов рук для постановки на учет в программно-технический комплекс (ПТК) ЦИАДИС-МВД в соответствующем федеральном округе в срок не более 10 дней с момента поступления следов рук, изъятых с мест преступлений. По резонансным преступлениям и в случаях, не терпящих отлагательств, – в возможно короткий срок.

Ведение федерального учета Централизованной дактилоскопической следотеки следов рук (ЦДС) осуществляется только в электронном виде с использованием электронных журналов регистрации объектов, поступивших на проверку и постановку на учет, с соблюдением требований информационной безопасности. ИК со следами рук, изъятыми с мест преступлений, подлежащие проверке и постановке на учет ЦДС, направляются в ЭКЦ МВД России только в электронном виде в 3-дневный срок после получения информации о результатах проверки по ПТК ЦИАДИС-МВД в соответствующем федеральном округе.

Информационные карты группируются по году совершения преступления в соответствии с нумерацией в Журнале регистрации объектов, поступивших на экспертно-криминалистический учет (приложение № 1 к Инструкции по организации использования экспертно-криминалистических учетов органов внутренних дел). При этом допускается их систематизация по времени, способу, виду совершения преступления и другим признакам, облегчающим поиск дактилоскопической информации.

Проверке по учету следов рук подлежат дактилокарты задержанных лиц, представляющих оперативный интерес, а также следы рук, изъятые с мест нераскрытых преступлений. Следы рук проверяются также по массивам дактилокарт соответствующего органа внутренних дел.

Линейные управления и отделы МВД России на железнодорожном, водном и воздушном транспорте направляют следы рук, изъятые в ходе осмотров мест происшествий, для проверки и постановки на

учет в соответствующие ЭКЦ УТ МВД России по ФО и ЛУ МВД России на транспорте. Дальнейшая проверка и постановка на учет следов рук осуществляется в соответствии с подп. 5.2 и 5.3 настоящего раздела.

Одновременно следы рук подлежат проверке в ЭКЦ территориального органа МВД России на региональном уровне, на территории которого совершено (выявлено) преступление.

При снятии следов рук с учета на бланке ИК делается отметка об основании снятия объекта с учета. В случаях, если на ИК установлены (идентифицированы) не все следы рук, ИК остаются в картотеке. В случае установления совпадения следов рук по региональной и межрегиональной базам данных дактилоскопической информации в ЭКЦ МВД России в течение 10 дней направляется информация о снятии ИК с учета.

Снятые с учета ИК помещаются в архив, срок хранения которых в архиве ИК составляет 5 лет. Работа по ведению и использованию учета следов рук отражается в Журнале регистрации объектов, поступивших на экспертно-криминалистический учет и Журнале регистрации объектов, поступивших на проверку по экспертно-криминалистическому учету. При этом сведения, внесенные в Журнал регистрации объектов, поступивших на экспертно-криминалистический учет, не вносятся в Журнал регистрации объектов, поступивших на проверку по экспертно-криминалистическому учету.

Примерный план занятия

1. Экспертно-криминалистические учеты ОВД РФ.
2. Информационные системы биометрической идентификации, используемые органами внутренних дел в борьбе с преступностью.

Вопросы для самоконтроля по теме

1. Какова основная форма ведения экспертно-криминалистических учетов?
2. Что относится к федеральным учетам?
3. Что относится к региональным учетам?
4. Что относится к местным учетам?
5. Как ведутся и используются учеты следов рук?

Перечень нормативных правовых актов, основной и дополнительной учебной литературы

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993.
2. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ.
3. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ.
4. О национальной платежной системе: федер. закон от 27.06.2011 № 161-ФЗ.
5. Об электронной подписи: федер. закон от 06.04.2011 № 63-ФЗ.
6. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента РФ от 17.03.2008 г. № 351.
7. О Плане счетов бухгалтерского учета для кредитных организаций и порядке его применения: положение Банка России от 27.02.2017 № 579-П.
8. О правилах осуществления перевода денежных средств: положение Банка России от 29.06.2021 № 762-П.
9. О рисках при дистанционном банковском обслуживании: письмо Банка России от 07.12.2007 № 197-Т.
10. Об организации использования экспертно-криминалистических учетов ОВД РФ: приказ МВД России от 10.02.2006 № 70.

Основная литература

1. Методы и способы получения доказательственной информации с электронных носителей: курс лекций / сост. А.В. Скачко. Краснодар: Краснодар. ун-т МВД России, 2014. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
2. Баркалова Ю.М Подготовка экспертов по производству компьютерных судебных экспертиз: метод. рекомендации. Воронеж: Воронежский институт МВД России, 2013. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
3. Криминалистика: учеб. / ред. А.Г. Филиппов. 3-е изд., перераб. и доп. М.: Юрайт, 2013.
4. Криминалистика. Углубленный курс: учеб. / ред. А.Г. Филиппов. М.: ДГСК МВД России, 2012.
5. Справочник следователя. Осмотр места происшествия / сост. А.В. Боловинов и др. М.: ЦОКР МВД России, 2010.

Дополнительная литература

1. Введенская О.Ю. Информационно-телекоммуникационная сеть Интернет как источник следовой информации о криминальном событии: фондовая лекция. Краснодар, КрУ МВД России, 2016. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
2. Еремченко В.И., Зиновьева Н.С., Алексеенко И.Л. Юридические и организационные аспекты использования информационно-телекоммуникационных систем в целях противодействия экстремистской деятельности в современных условиях: науч.-практ. пособие. Краснодар: Краснодар. ун-т МВД России, 2015.
3. Першин А.Н. Криминалистические основы анализа документированной информации в уголовном судопроизводстве. Омск: Омская академия МВД России, 2015. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
4. Стельмах В.Ю. Получение информации о соединениях между абонентами и(или) абонентскими устройствами как следственное действие. Екатеринбург: Уральский юридический институт МВД России, 2014. Режим доступа: Электронная библиотека КрУ МВД России, требуется авторизация: <http://libkrumvd.ru>
5. Судебные экспертизы в гражданском судопроизводстве: организация и практика: науч.-практ. пособие / ред. Е.Р. Россинская. М.: Юрайт, 2011.
6. Тактика следственных действий, направленных на отыскание, обнаружение и исследование электронных носителей и информации на них: учеб. пособие / ред.: А.А. Кузнецов, Д.В. Муленков. Омск: Омская академия МВД России, 2015.

Оглавление

Предисловие.....	3
Принятые сокращения.....	5
1. Общие положения противодействия преступлениям в сфере информационно-коммуникационных технологий.....	6
Тема 1.1. Правовое регулирование общественных отношений в сфере информации, информационных технологий и защиты информации.....	6
Тема 1.2. Уголовно-правовая характеристика и квалификация преступлений, совершаемых с использованием информационно-коммуникационных технологий.....	24
Тема 1.3. Криминалистическая и криминологическая характеристики преступлений, совершаемых с использованием информационно-коммуникационных технологий.....	29
Тема 1.4. Современное состояние борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий.....	37
Тема 1.5. Организация профилактической работы по предупреждению преступлений, совершаемых с использованием информационно-коммуникационных технологий.....	43
Тема 1.6. Международный опыт противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.....	50
2. Оперативно-розыскная деятельность как основа выявления и раскрытия преступлений.....	58
Тема 2.1. Понятие и сущность оперативно-розыскной деятельности...	58
Тема 2.2. Задачи и принципы оперативно-розыскной деятельности...	64
Тема 2.3. Правовое регулирование оперативно-розыскной деятельности.....	69
Тема 2.4. Соблюдение прав и свобод человека и гражданина при осуществлении оперативно-розыскной деятельности.....	75
Тема 2.5. Государственные органы и должностные лица, осуществляющие оперативно-розыскную деятельность, их обязанности и права.....	82
Тема 2.6. Лица, оказывающие конфиденциальное содействие (сотрудничество) органам внутренних дел.....	93

Тема 2.7. Оперативно-розыскные мероприятия и их характеристика.....	100
Тема 2.8. Оперативно-розыскные мероприятия, ограничивающие конституционные права граждан.....	103
Тема 2.9. Основания и условия проведения оперативно-розыскных мероприятий.....	116
Тема 2.10. Информационное обеспечение оперативно-розыскной деятельности.....	121
Тема 2.11. Особенности документирования оперативно-розыскной деятельности органов внутренних дел при раскрытии преступлений.....	126
Тема 2.12. Использование результатов оперативно-розыскной деятельности.....	138
Тема 2.13. Взаимодействие оперативных подразделений органов внутренних дел с другими субъектами оперативно-розыскной деятельности и иными государственными органами.....	144
Тема 2.14. Взаимодействие оперативных подразделений с органами предварительного следствия и дознания.....	155
Тема 2.15. Контроль и надзор за оперативно-розыскной деятельностью.....	159
3. Общие положения по расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий.....	168
Тема 3.1. Действия сотрудников органов внутренних дел при поступлении заявлений (сообщений) о преступлениях, совершенных с использованием информационно-коммуникационных технологий.....	168
Тема 3.2. Особенности возбуждения уголовных дел по преступлениям, совершаемым с использованием информационно-коммуникационных технологий.....	180
Тема 3.3. Электронный носитель информации как техническое средство, содержащее значимую для уголовного дела информацию.....	183
Тема 3.4. Производство отдельных следственных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий.....	186
Тема 3.5. Участие специалиста при проведении отдельных оперативно-розыскных мероприятий и следственных действий по преступлениям, совершаемым с использованием информационно-коммуникационных технологий.....	206

Тема 3.6. Криминалистическое исследование электронных носителей информации, особенности подготовки и назначения судебных экспертиз по уголовным делам о преступлениях, совершаемых с использованием информационно-коммуникационных технологий.....	212
4. Организация противодействия общеуголовным, экономическим и преступлениям террористической и экстремистской направленности, совершаемым с использованием информационно-коммуникационных технологий.....	219
Тема 4.1. Выявление и раскрытие преступлений общеуголовной направленности, совершаемых с использованием информационно-коммуникационных технологий.....	219
Тема 4.2. Выявление и раскрытие преступлений экстремистской и террористической направленности, совершаемых с использованием информационно-коммуникационных технологий.....	233
Тема 4.3. Понятие и сущность криптовалют и других виртуальных активов.....	242
5. Организация противодействия преступлениям по линии незаконного оборота наркотиков, совершаемым с использованием информационно-коммуникационных технологий.....	253
Тема 5.1. Противодействие незаконному обороту наркотиков, совершаемому с использованием информационно-коммуникационных технологий.....	253
Тема 5.2. Технические возможности использования биллинговых данных при раскрытии и расследовании уголовных дел, связанных с незаконным оборотом наркотиков. Правовая база для использования в раскрытии тяжких и особо тяжких преступлений системы технических средств по обеспечению оперативно-розыскных мероприятий. Понятие и принципы функционирования базовой станции.....	257
Тема 5.3. Тактика противодействия незаконным наркооперациям, совершаемым с использованием блокчейн-технологий.....	265
Тема 5.4. Особенности раскрытия преступлений в сфере оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий.....	269
Тема 5.5. Взаимодействие оперативных и экспертно-криминалистических подразделений при раскрытии и расследовании преступлений по линии незаконного оборота наркотиков, совершаемых с использованием информационно-коммуникационных технологий.....	277

6. Организация противодействия преступлениям в сфере коммуникаций и компьютерной информации.....	286
Тема 6.1. Особенности выявления и раскрытия преступлений в сфере коммуникаций и компьютерной информации.....	286
Тема 6.2. Выявление и раскрытие преступлений, совершаемых в системе дистанционного банковского обслуживания.....	291
Тема 6.3. Выявление фактов вовлечения несовершеннолетних в деструктивную деятельность посредством информационно-коммуникационных технологий.....	300
Тема 6.4. Использование биометрических технологий и методов, способствующих раскрытию преступлений.....	310

Учебное издание

**Актуальные вопросы деятельности подразделений,
специализирующихся на предотвращении, выявлении, раскрытии
и расследовании преступлений, совершаемых с использованием
информационно-коммуникационных технологий**

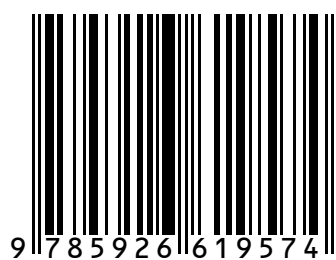
Учебное пособие

Составители:

Афанасьев Евгений Владимирович,
Башинская Инна Геннадьевна,
Бевз Сергей Олегович и др.

Редакторы: *М. В. Краснобаева, В. С. Ревина*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1957-4



Подписано в печать 26.01.2023. Формат 60x84 1/16.
Усл. печ. л. 18,8. Тираж 100 экз. Заказ 103.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.