Министерство внутренних дел Российской Федерации
Краснодарский университет

В.И. Еремченко, Н.С. Зиновьева

КИБЕРНЕТИКА: ЕЕ ЗНАЧЕНИЕ И ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ В СОВРЕМЕННОЙ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ СТРУКТУР

Учебное пособие

Краснодар
КрУ МВД России
2015

УДК 343.985
ББК 67.52
Е70

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:

Д.Н. Лозовский, доктор юридических наук (Краснодарский университет МВД России)

Д.Н. Фокин (Следственная часть Следственного управления УМВД России по г. Краснодару).

Еремченко В.И., Зиновьева Н.С.

Е70 Кибернетика: ее значение и возможности использования в современной деятельности правоохранительных структур: учебное пособие / В.И. Еремченко, Н.С. Зиновьева. – Краснодар: Краснодарский университет МВД России. 2015. – 80 с.

ISBN:

Учебное пособие раскрывает закономерности механизма передачи, хранения и переработки информации, содержащейся на информационных порталах социальных сетей и электронных почтовых услуг, размещенных в глобальной информационно-телекоммуникационной системе Интернет, а также образующейся в результате пользования услугами современных сотовых операторов связи. Даны рекомендации сотрудникам правоохранительных органов по использованию возможностей как социальных сетей и электронной почты Интернета, так и сотовых операторов связи в раскрытии, расследовании и предотвращении преступлений. Представлены выводы и вынесены предложения по совершенствованию как организационных моментов раскрытия и расследования преступлений, так и законодательной базы, регламентирующей разбираемую сферу телекоммуникаций.

Ориентировано на использование в образовательных организациях системы МВД России в ходе подготовки специалистов и повышения квалификации практических сотрудников, а также в практической деятельности следственных и оперативных подразделений.

УДК 343.985
ББК 67.52

ISBN:

ОГЛАВЛЕНИЕ

Введение.....4

Глава 1. Современная кибернетика и ее связь с криминалистикой - наукой о раскрытии, расследовании и предотвращении преступлений.....7

1.1. Кибернетика как наука.....7

1.2. Кибернетика как источник криминалистики.....15

Глава 2. Кибернетизация современной жизни как источник криминалистически значимой информации.....23

2.1. Социальные сети и их использование в деятельности следователя.....23

2.2. Сотовая связь в раскрытии и расследовании преступлений.....36

2.3. Электронная почтовая связь, как безмолвный свидетель.....48

Заключение.....59

Список использованных источников.....64

Приложения.....70

ВВЕДЕНИЕ

Повышение эффективности деятельности сотрудников по раскрытию, расследованию и предупреждению преступлений невозможно без внедрения современных достижений науки и техники, информационных систем, сетей связи, а также современных информационно-телекоммуникационных инфраструктур. Изменение и конкретизация основных обязанностей полиции дает возможность полагать, что деятельность по изучению методов розыска скрывшихся подозреваемых, выявлению доказательств совершенных преступлений в социальных сетях, использованию телекоммуникационных ресурсов для формирования доказательственной базы, поиску интересующих субъектов при помощи сотовых операторов связи является актуальной и требует более глубокого изучения и продуктивного применения в решении профессиональных задач сотрудников органов внутренних дел.

Мы живем в 21 веке – веке высоких информационных технологий. Нынешнее время разительно отличается от предыдущего: это период, характеризующийся небывалым ростом объема информационных потоков. То, что еще совсем недавно казалось новым и неизведанным, сегодня уже стало обыденностью. Одними из основных достижений современного человечества явилось создание единой информационной сети Интернет и, конечно же, мобильного сотового телефона, который можно считать радиомаяком, позволяющим определить местоположение его владельца. Глобальная паутина Интернет стала всеобъемлющим пространством, которое объединило всё и вся, поставила в зависимость деятельность человека, систему ценностей и значимость культурного досуга. Как и любая другая кибернетическая система, информационная сеть Интернет и сотовые связи подчиняется определенным закономерностям по управлению, передаче, хранению и переработки информации. Наличие указанных закономерностей позволяет говорить о возможности их

использования ни только в реализации изначально поставленных целей, но также и в достижении альтернативных целей. Значительное увеличение числа людей занятых информационными технологиями, коммуникациями, и владеющими мобильными сотовыми телефонами, к примеру, предоставляет возможность органам внутренних дел разыскивать скрывшихся подозреваемых, выявлять доказательства совершенных преступлений, а также устанавливать дополнительных участников «темных дел» причастных или непосредственно главенствующих в совершённых преступлениях, анализировать преступную группу и причину преступлений. О возможности использования современных телекоммуникационных систем уже неоднократно отмечалось разными учеными[1], однако сам механизм их использования до сих пор не получил надлежащей огласки, а также имеет ряд проблем, которые требуют разрешения на законодательном уровне. Разрешение данных проблем, а также ряда других смежных вопросов реализовано в рамках представленного учебного пособия.

В представленном пособии, на основании комплексного исследования кибернетики и ее взаимосвязи с криминалистикой, возможностей и необходимости использования современных достижений науки и техники, информационных систем, сетей связи, а также современных информационно-телекоммуникационных инфраструктур в профессиональной деятельности сотрудников органов внутренних дел, представлены пути реализации разного рода служебных задач правоохранительных органов при помощи знания законов кибернетики (законов информационных потоков).

Результаты, изложенные в данном труде, основаны на фундаментальных исследованиях в области криминалистики,

[1] См.: Гончарова Е.А. Использование сети интернет в раскрытии и расследовании преступлений // Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Юридические науки». Т. 22 (61). №1. 2009. с. 310-315.

информатики, математики, логики, уголовного права и уголовно процесса. Учебный материал представлен с учетом анализа научных трудов таких ученых, как Р.С. Белкин, Л.Т. Кузин, А.И. Винберг, Г.Л. Грановский, В.И. Гончаренко, Г.Г. Зуйков, З.И. Кирсанов, В.Н. Кудрявцев, И.Д. Кучеров, И.М. Лузгин, В.С. Митричева, В.Ф. Орлова, А.Р. Ратинов, Н.А. Селиванов, А.А. Эйсман, Р.Э. Эльбур, И.В. Яковенко, С.Н. Шабунин, В.А. Галкин, Ю.А. Григорьев, В.В. Абакумов и А.А. Голубев.

Кроме того, наряду с теоретической базой, в работе также использованы и эмпирические источники, к таковым следует отнести судебную и следственную практику по уголовным делам, основанным на использовании информационно-телекоммуникационных источников доказательственной информации в раскрытии, расследовании и предотвращении преступлений, а также результаты анкетирования сотрудников следственных подразделений, осуществляющих свою профессиональную деятельность на территории Краснодарского края.

Таким образом, использование данного учебного пособия может быть полезно как в процессе подготовки будущих специалистов органов внутренних дел, так и при разрешении некоторых служебных задач в повседневной деятельности следователя и оперативного уполномоченного.

ГЛАВА 1. СОВРЕМЕННАЯ КИБЕРНЕТИКА И ЕЕ СВЯЗЬ С КРИМИНАЛИСТИКОЙ – НАУКОЙ О РАСКРЫТИИ, РАССЛЕДОВАНИИ И ПРЕДОТВРАЩЕНИИ ПРЕСТУПЛЕНИЙ

1.1. Кибернетика как наука

Кибернетика - это фундаментальный труд, который описывает главные понятия и принципы управления информации. Фронт современной науки простирается от сравнительно частных, конкретных концепций относительно различных областей физического и химического мира, до всеохватывающих теорий, объемлющих различные сферы природы, общества и технической деятельности человека. Кибернетика имеет разветвленную систему и многозначное понимание кибернетики, которое разница в зависимости от той науки, в которой она используется. На современном этапе развития понимание кибернетики можно встретить в таких областях научного знания, как:

- биология;
- инженерия;
- психология;
- экономика и управление;
- математика;
- социология;
- кибернетика и т.д.

Так, к примеру, в биологии под понятием «кибернетика» принято понимать исследование кибернетических систем в биологических организмах; в инженерии – используют это понятие, чтобы проанализировать отказы систем, в которых маленькие ошибки и недостатки могут привести к сбою всей системы; в психологии – устанавливают при помощи кибернетики структурно-функциональную

организацию взаимодействия различных анализаторных систем, сфер сознания и подсознания в процессе формирования поведения, в процессе взаимодействия людей между собой, с техническими, экологическими, социальными системами.

Нас же будет интересовать рассмотрение кибернетики как науки об общих закономерностях процессов управления и передачи информации в технических, биологических и социальных системах.

Для управления в общем смысле термин «кибернетика» впервые употребил в своих сочинениях древнегреческий философ Платон. Исторически сложившаяся совокупность сочинений «Платоновский корпус» определяет «кибернетику» в одном случае как искусство управления кораблями и колесницами, в другом случае, под этим понятием понималось искусство управления людьми. Действительное становление кибернетики как науки произошло в 1948 г., американский ученый Норберт Винер опубликовал книгу «Кибернетика, или управление и связь в животном и машине»[1], обобщив в ней закономерности, относящиеся к системам управления различной природы – биологическим, техническим и социальным. В книге «Кибернетика и общество»[2], изданной в 1954 году Винером подробно были рассмотрены задачи связанные с управлением в социальных системах. Век прогресса и торжества разума – XX век, принёс серьёзные изменения в мировоззрении, интересах и деятельности людей, стремительное развитие вычислительной техники породило большой интерес к кибернетике как науки и вызвало бурное развитие во всем мире. В 80-90е годы термин «кибернетика» был частично вытеснен термином «информатика», имеющим отношение, прежде всего, к компьютерам и обработке информации. В связи с развитием Интернета, а именно киберпространства и устройств с высокой степенью физического и

[1] См.: Винер Н. Кибернетика, или управление и связь в животном и машине. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – 344 с.

[2] См.: Винер Н. Кибернетика и общество. – М.: Издательство иностранной литературы, 1958. – 200 с.

интеллектуального взаимодействия человека и технических средств автоматики, рассматриваемый термин вновь стал популярен. Кибернетика как наука изучает не вещественный состав систем и не их структуру, а результат работы данного класса систем и именно это является ее спецификой.

Предметом кибернетики как науки являются закономерности объективной действительности, отображающиеся в различных явлениях, процессах, которые смело можно отнести к кибернетическим системам управления. Кибернетической системой считается та, в которой выполнены два ключевых условия: сложность и динамичность. Каждое явление объективной закономерности обладает определенной степенью сложности, что позволяет отследить процессы управления. Процессы управления в озвученных закономерностях имеют смысл быть, если эта система изменяется, движется, т.е. является динамической системой. В свою очередь объектом изучения кибернетики являются сложные динамические системы. Как правило, к сложным динамическим системам относятся:

- животные;
- растения;
- организованные группы людей;
- государство;
- отрасли промышленности;
- транспортные средства;
- сотовая связь;
- единая сеть Интернет и т.п.

Рассматривая сложные динамические системы, а именно организмы, социально-экономические комплексы и технические агрегаты, кибернетика не ставит перед собой задач полного, конкретного изучения их функционирования, она изучает общие закономерности управляющих систем, их конкретные физические особенности находятся вне поля ее

зрения. На примере исследования мощной электростанции, являющейся сложной динамической системой, можно проследить, что кибернетика как наука не фокусирует свое внимание непосредственно на вопросе о коэффициенте ее полезного действия, габаритах генераторов, физических процессах генерирования энергии, а интересуется тем какие логические функции выполняются при работе электростанции и ее устройств, как они участвуют в процессах управления. Изучая, наконец, с кибернетической точки зрения взаимодействие внутри некоторой социальной группы, мы не придаем значения биофизическим и биохимическим процессам, происходящим внутри организма каждого из индивидуумов, образующих данный коллектив.

Предмет изучения кибернетики представлен кибернетическими системами, в которых заложен процесс управления, т.е. процесс сбора, обработки, хранения информации и дальнейшего ее использования в целях управления. Если иные частные процессы вмешиваются в процессы управления системой, кибернетика должна включать их в сферу своего исследования, но не всестороннего, а именно с позиций их воздействия на процессы управления. Кибернетика охватывает все науки, но не полностью, а лишь в той их части, которая относится к сфере процессов управления, связанных с этими науками и соответственно с изучаемыми ими системами. Таким образом, можно прийти к выводу, что предметом изучения кибернетики являются процессы управления в сложных динамических системах.

Основными задачами кибернетики выступают:

1) установление фактов, общих для управляемых систем или для некоторых их совокупностей;

2) выявление ограничений, свойственных управляемым системам и установление их происхождения;

3) нахождение общих законов, которым подчиняются управляемые системы;

4) определение путей практического использования установленных фактов и найденных закономерностей.[1]

В «Кибернетическом» подходе к системам существует ряд основных понятий: управление, управляющая система, управляемая система, организация, обратная связь, алгоритм, модель, оптимизация, сигнал и другие. Понятие «управление» можно определить для систем любой природы, в качестве воздействие на объект, выбранное на основании имеющейся для этого информации из множества возможных воздействий, изменяющее его функционирование или развитие. У управляемых систем всегда существует некоторое множество возможных изменений, из которого производится выбор предпочтительного изменения, отсутствие выбора исключает процесс управления.

Управление - это вызов изменений в системе или перевод системы из одного состояния в другое в соответствии с объективно существующей или выбранной целью.

Управлять - это и предвидеть те изменения, которые произойдут в системе после подачи управляющего воздействия (сигнала, несущего информацию). Любая система управления рассматривается лишь в совокупности, единстве управляющей системы то есть субъекта управления и управляемой системы – объекта управления, происходящие во внешней среде. Управление системой или объектом всегда происходит в какой-то внешней среде. Управление во внешней среде системой, а именно поведение любой управляемой системы всегда рассматривается с учетом окружающей. Ведь происходит влияние друг на друга всех объектов, явлений и процессов, однако, выделяя какой-либо объект, необходимо учитывать влияние среды на этот объект и наоборот. Организованность системы позволяет полагать, что она имеет свойство управляемости, ведь именно организованность дает потенциальную

[1] См.: Розанова Л.В. Основы кибернетики: Конспект лекций. – Омск: Изд-во ОмГТУ, 2009. – с.6.

возможность управления.

Чтобы управление могло функционировать, то есть целенаправленно изменять объект, оно должно содержать четыре необходимых элемента:

1. каналы сбора информации о состоянии среды и объекта;

2. канал воздействия на объект;

3. цель управления;

4. способ (алгоритм, правило) управления, указывающий, каким образом можно достичь поставленной цели, располагая информацией о состоянии среды и объекта.[1]

Управление – информационный процесс, в свою очередь информация это ресурс управления. В связи с этим кибернетика – наука об информации, об информационных системах и процессах.

Самый исходный смысл термина «информация» связан со сведениями, сообщениями и их передачей. Бурное развитие в нашем веке телефона, телеграфа, радио, телевидения и других средств массовой коммуникации потребовало повышения эффективности процессов передачи, хранения и переработки передаваемых в сообщении информации. «Докибернетическое» понятие информации связано с совокупностью сведений, данных и знаний. Оно стало явно непонятным, неопределенным с возникновением кибернетики. Понятие информации в кибернетики уточняется в математических «теориях информации». Это теории статистической, комбинаторной, топологической, семантической информации.

В отечественной и зарубежной литературе предлагается много разных концепций (определений) информации:

- информация как отраженное разнообразие;

- информация как устранение неопределенности (энтропии);

- информация как связь между управляющей и управляемой

[1] См.: Глазков Ю.Н. Кибернетика и синергетика – науки о самоорганизующихся системах: Контрольная работа – 2000. – с.6.

системами;

- информация как преобразование сообщений;

- информация как единство содержания и формы (например, мысль – содержание, а само слово, звук – форма);

- информация – это мера упорядоченности, организации системы в ее связях с окружающей средой.[1]

Общее понятие информации должно непротиворечиво охватывать все определения информации, все виды информации.

Информация может быть структурной, застывшей, окостенелой. Например, в минералах, машинах, приборах, автоматических линиях. Любая машина – это овеществленная научная и техническая информация, разум общества, ставший предметом.

Информация может быть также функциональной, «актуальным управлением». Информация измеримая величина. Она измеряется в битах.

Кроме того, информация обладает рядом свойств:

- способностью управлять физическими, химическими, биологическими и социальными процессами. Там, где есть информация, действует управление, а там, где осуществляется управление, непременно наличествует и информация;

- способностью передаваться на расстоянии (при перемещении инфоносителя);

- способностью подвергаться переработке;

- способностью сохраняться в течение любых промежутков времени и изменяться во времени;

- способностью переходить из пассивной формы в активную. Например, когда извлекается из «памяти» для построения тех или иных структур (синтез белка, создание текста на компьютере и т. д.).[2]

---

[1] См.: Рутковская М.В. Проблемы информации в поле кибернетики // Философские проблемы информационных технологий и киберпространства. 2010. №1. с.194.

[2] См.: Хакин Г. Синергетика. Иерархии неустойчивостей в самоорганизующихся системах и устройствах: Монография. – Москва: Изд-во Мир, 1985. – 424 с.

Информация существенно влияет на ускоренное развитие науки, систем управления, техники и различных отраслей народного хозяйства. Информация – неисчерпаемый ресурс общества, является первоосновой мира, всего сущего. Современным научным обобщением всех информационных процессов в природе и обществе явилась информациология – генерализованная наука о природе информации и законах информации.

Основная задача кибернетики – достижение на основе присущих ей методов и средств оптимального уровня управления, т.е. принятие наилучших управленческих решений. Таким образом, кибернетическим называется такое управление, которое:

- рассматривает организацию как некоторую большую систему, каждый элемент которой берется не только сам по себе, но и как часть большой совокупности, в которую он входит;

- обеспечивает оптимальное решение многовариантных динамических задач организации;

- использует специфические методы, выдвинутые кибернетикой (обратную связь, саморегулирование и самоорганизацию и т.п.);

- широко применяет механизацию и автоматизацию управленческих работ на основе использования вычислительной и управляющей техники и компьютерных технологий.

Из кибернетики управление заимствует ряд законов и принципов. К таковым могут быть отнесены:

- закон необходимого разнообразия;

- принцип эмерджентности;

- принцип внешнего дополнения;

- закон обратной связи;

- принцип выбора решения;

- принцип декомпозиции;

- принципы иерархии управления и автоматического регулирования.[1]

Все указанные законы и принципы кибернетики взаимосвязаны и взаимообусловлены. Они должны непременно учитываться при организации структуры как объекта, так и субъекта управления, а в равной мере при реализации временного аспекта их организации, т.е. при осуществлении процессов планирования и управления.

В завершении параграфа важно отметить, что в настоящее время не существует единого понимания кибернетики. Не смотря на это, в течение времени она смогла сформироваться в отдельную науку со своими задачами, законами и принципами, имеющими разветвленные направления в различных областях знаний биологии, математики, медицины, информатики, психологии, физики, химии и других наук, объединенных при исследовании управления системами.

1.2. Кибернетика как источник криминалистики

Криминалистика - комплексная наука, систематизирующая в себе многие области знаний. Она использует определенные положения других наук, в том числе естественных и технических.

К источникам криминалистики, которые заложили ее формирование как науки и повлияли на ее дальнейшее развитие, можно отнести:

- уголовное право;
- уголовно-процессуальное право;
- криминологию;
- оперативно-розыскную теорию;
- теорию управления;
- юридическую психологию;

[1] См.: Абакумов В.В., Голубев А.А., Кустарев В.П., Подлесных В.И., Прохоров Ю.К., Тюленев Л.В. Электронный учебник по дисциплине: «Менеджмент» - СПбГУ ИТМО, кафедра менеджмента. Режим доступа: http://de.ifmo.ru/bk_netra/page.php?tutindex=3&index=16

- этику;

- логику;

- математику;

- физику;

- химию и т.д.

Таким образом, формирование криминалистики как науки, а также ее дальнейшее развитие обусловили не только нормы уголовного и уголовно-процессуального права, устанавливающие общую процедуру расследования преступлений и изъятия оперативной информации, но и также ряд естественных наук: математика, рассматривающая «пространственные формы и количественные отношения действительного мира» (Ф. Энгельс); физика, изучающую наиболее общие свойства материального мира; химия, познающая превращения веществ, сопровождающиеся изменением их состава и строения; метеорология – наука о земной атмосфере и происходящих в ней процессах; биология; генетика, и, конечно же, кибернетика как техническая наука о закономерностях управления, передачи хранения, и переработки информации.

Эффективное использование в раскрытии и расследовании преступлений средств электронно-вычислительной, электронно-оптической техники, видеозаписи доказывают их возможности в обнаружении, фиксации, передаче и хранении криминалистической информации и необходимость дальнейшего совершенствования как самих технических средств, так и методов их использования. Все более широкое применение получают компьютерные технологии, позволяющие быстро и с высоким качеством изготавливать субъективные портреты, фототаблицы к протоколу следственного действия, снятые на видеокамеру, осуществлять поисковые действия в автоматизированных системах и т.п.[1]

[1] См.: Филиппов А.Г., Агафонов В.В. Криминалистика: конспект лекций. – Москва., 2009. Режим доступа: http://lib.rus.ec/b/204003

Дальнейшее развитие науки и техники в целях раскрытия и расследования преступлений, мы можем предположить, направлено также на эффективное использование сотрудниками органов внутренних дел методов по розыску скрывшихся подозреваемых, выявлению доказательств совершенных преступлений в социальных сетях, поиску субъектов при помощи сотовых операторов связи и получение информации с электронной почты, используя общие законы кибернетики (закон информационных потоков). Ведь 74 % опрошенных сотрудников следственных органов Краснодарского края, действительно считают, что реализация разного рода служебных задача невозможна без внедрения современных достижений и знания информационных потоков (см. прил.1)

Научно-техническая революция создала реальные условия для расширения диапазона разных наук. Особое место среди них занимают науки и научные направления кибернетического профиля.

В связи с этим целесообразно рассмотреть одно из основных определений предмета криминалистики, обозначенное в 1967 году Р.С. Белкиным: объектом познания криминалистики являются закономерности, в частности закономерности собирания, исследования, оценки и использования доказательств и основанные на их познании средства и методы судебного исследования и предотвращения преступлений[1]. Действительно, в качестве основного объекта познания криминалистики, обозначенного Р.С. Белкиным, являются объективные закономерности, ведь в науковедческой литературе давно уже принято за истину, что важнейшей чертой любой науки, а в частности научного направления кибернетического профиля, является изучение соответствующих законов и закономерностей. Тогда как познание вообще есть необходимый признак сознательной практической деятельности в любой области. Следовательно, криминалистика как наука может и должна исследовать соответствующие

[1] См.: Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учеб. для вузов / под ред. проф. Р.С. Белкина. – М.: НОРМА-ИНФРА, 2000. – с. 49-59.

объективные закономерности. Важно только правильно определить их характер, объем и направление исследования. Р.С. Белкин утверждает что, в качестве основного объекта познания криминалистики выступают закономерности собирания, исследования, оценки и использования судебных доказательств.

На наш взгляд, при проведении неотложных и первоначальных следственных действий, а тем более при проведении оперативно-розыскных мероприятий и криминалистических экспертиз мы имеем дело не с судебными доказательствами, а с информацией, в отношении которой на первом этапе расследования лишь предполагается, что она относится к событию преступления и преступнику (назовем такую информацию криминалистической) с ее носителями и непосредственными источниками. Поэтому при определении предмета криминалистики, а следовательно, и криминалистической кибернетики следует говорить не о закономерностях возникновения судебных доказательств и работы с ними, а о закономерностях возникновения криминалистической информации и построения наиболее оптимальной технологии и тактики проведения информационных процессов, т.е. процессов выявления, сбора, хранения, переработки, передачи и использования информации о событии преступления и преступнике, а также об особенностях методики их проведения с учетом характера расследуемого преступления[1]. Именно теоретические и методологические основы разработки технологии и тактики проведения информационных процессов и особенности их построения с учетом характера расследуемого уголовного дела, а также проблемы разработки и использования наиболее совершенных средств и методов, обеспечивающих раскрытие и расследование преступлений, составляют ядро криминалистики как науки, а практическая их реализация – основу одного из аспектов деятельности по борьбе с преступностью –

[1] См.: Игошин В.В. Интегральная природа науки криминалистики и ее проявление в криминалистической технике: дисс. … канд. юрид. наук. Ижевск, 2005. 192 с.

информационно-познавательного.

На наш взгляд, совершенно правильно рассматривают этот аспект как самостоятельный уровень уголовно-процессуального доказывания. Так, В.Я. Колдин полностью придерживается такой позиции. По его мнению, предметом криминалистики является информационно-познавательная структура расследования.

Весьма интересны и заслуживают пристального внимания соображения о предмете криминалистики, высказанные А.А. Эйсманом. Он, в частности, пришел к выводу о том, что к объектам, изучаемым криминалистикой, относятся две группы взаимосвязей и взаимодействия: «...взаимосвязи и взаимодействия материальных объектов (сфера криминалистической техники) и взаимодействия и отношения людей (сфера тактики и частной методики)»[1]. При таком подходе к предмету криминалистики нельзя не заметить влияния идей кибернетики, общей теории систем и системного подхода, использование которых открывает большие возможности в плане изыскания путей дальнейшей оптимизации криминалистической деятельности и повышения эффективности ее функционирования как информационно-функциональной системы. Следует также отметить, что в ходе расследования того или иного преступления мы действительно имеем дело не с изолированными друг от друга объектами, а с системами объектов, между которыми существуют определенные взаимосвязи, которые между собой взаимодействуют или ранее взаимодействовали. Естественно, что выявление и познание природы таких связей, определение характера и особенностей взаимодействующих объектов – одна из важных задач расследования, а применительно к предмету криминалистики – один из его элементов.

---

[1] См.: Селиванов Н.А., Танасевич В.Г., Эйсман А.А. Советская криминалистика. Теоретические проблемы. – Москва: Юридическая литература, 1978. Режим доступа: http://зачётка.рф/book/4357/189390/%C2%A7%201.%20%D0%9F%D1%80%D0%B5%D0%B4%D0%BC%D0%B5%D1%82%20%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B8.html

Основой криминалистической кибернетики является творческое использование математического аппарата, идей и технических средств кибернетики в целях разработки наиболее оптимальных методик алгоритмизации и автоматизации информационных процессов в сфере деятельности по раскрытию и расследованию преступлений. Криминалистическая кибернетика – это самостоятельное направление в теории и практике советской криминалистики, ее частная теория, целевой функцией которой является исследование закономерностей, общенаучных предпосылок, и конкретных условий использования математического аппарата, идей и технических средств кибернетики и разработка на их основе специальных методов и алгоритмов решения криминалистических задач, а также построения и использования автоматизированных информационных систем, призванных оптимизировать и повысить эффективность деятельности по раскрытию, расследованию и предупреждению преступлений.

Более кратко сущность и предмет криминалистической кибернетики можно выразить так: криминалистическая кибернетика – это частная криминалистическая теория, которая по своей природе является комплексной отраслью знания об общих закономерностях и конкретных методах математизации и автоматизации информационных процессов в сфере деятельности по раскрытию и расследованию преступлений, разрабатываемых и используемых в целях ее оптимизации и повышения эффективности функционирования как кибернетической системы. Разумеется, ни то, ни другое определение не претендуют на исчерпывающее раскрытие всего содержания и всех признаков определяемого понятия, поскольку любая дефиниция, как известно, обедняет действительное содержание определяемого.

По мере дальнейшего расширения и углубления исследований проблем, связанных с использованием математического аппарата и средств вычислительной техники в сфере криминалистической деятельности, т.е.

ее математизации и кибернетизации, будут выявляться их новые формы и направления. В силу этого и само понятие криминалистической кибернетики, и ее предмет будут наполняться все более глубоким и конкретным содержанием, а ее роль постоянно возрастать.

Помимо использования достижений кибернетики в целях самоорганизации и оптимизации самого процесса по выявлению, раскрытию и расследованию преступлений, криминалистика также нацелена на использование разработанных кибернетикой представлений об управлении и обмене информацией в различных областях. Наибольшую актуальность в последнее время приобретают новые источники получения доказательственной базы, имеющие техническую природу и разработанные в иных целях, но используемых криминалистикой для решения поставленных перед ней задач.

К таковым источникам доказательственной базы могут быть отнесены:

- дислоцированные во всемирной паутине Интернет социальные сети как система накопления и обмена информацией;

- электронная почтовая система обмена сообщениями и иной электронной информацией в сети Интернет;

- система сотовой подвижной связи.

Именно эти источники выступают некой базой, аккумулирующей в себе колоссальный объем информации о субъектах нашего общества, их идентификационных данных, увлечениях, дислокации, занятиях, круге общения и т.п. Именно эта информация может иметь незаменимое значение в правоохранительной деятельности.

Однако, не смотря на кажущуюся доступность таковых сведений, их надлежащее процессуальное получение может оказаться весьма затруднительным без обладания правоохранительным сотрудником представлений об организации процессов хранения и обмена информацией в рассматриваемых системах. Изучение данных положений позволит

расширить границы знания сотрудников, которые не имеют представления об указанных положениях в связи с недостаточным профессиональным уровнем, который составляет среди анкетированных сотрудников 22 %. (см. прил.1). В связи с чем, представленное учебное пособие нацелено на формирование наглядного представления о процессах в данных системах, которое могло бы быть использовано как практическими сотрудниками правоохранительных органов, так и учащимися высших учебных заведений в целях изучения использования достижений современных кибернетических технологий в выявлении, раскрытии и расследовании преступлений.

Таким образом, кибернетика как источник криминалистики оказывает на нее влияние в двух сферах:

1. Используя достижения кибернетики, позволяет оптимизировать себя как управляемую структуру, а именно саму организацию процесса по выявлению, раскрытию и расследованию преступлений;

2. Используя знания о принципах передачи, хранения и переработки информации в системах, формирует представление об организации процесса получения криминалистически значимой информации из данных систем (к таковым может быть отнесена информационно-телекоммуникационная система Интернет, социальные сети и электронные почтовые ресурсы как составные элементы Интернета, система сотовой связи и т.п.).

ГЛАВА 2. КИБЕРНЕТИЗАЦИЯ СОВРЕМЕННОЙ ЖИЗНИ КАК ИСТОЧНИК КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

2.1. Социальные сети и их использование в деятельности следователя

Интернет – это глобальная компьютерная сеть, охватывающая весь мир, имеющая более 2,4 млрд. абонентов в более чем 150 странах мира. Количество пользователей стремительно растет во всем мире и моду на него диктует век высоких информационных технологий. Ежемесячно оно увеличивается на 7-10%[1]. Глобальная паутина стала всеобъемлющим пространством, которое объединило всё и вся, поставила в зависимость деятельность человека, систему ценностей и значимость культурного досуга. Действительно, с появлением Интернета многие аспекты нашей жизни постепенно перекочевали в виртуальный мир, и общение не стало исключением, скорее, даже наоборот. Потребность человека в скоростном общении (передаче информации) и стало основанием для появления Интернета. И если несколько лет назад Интернет, прежде всего, являлся источником обмена информацией в обезличенном виде, то уже сегодня у большинства людей эта глобальная сеть ассоциируется с общением и обменом информацией между конкретными людьми. Так 34 % анкетированных сотрудников считаю интернет мощным ресурсом получения оперативной информации, объединивший огромное количество людей (см. прил.1). В реалиях настоящего времени можно сказать, что социальные сети, обеспечивающие контакты между людьми, образуют ядро современного Интернета.

Главной причиной, породившей создание социальных сетей, обеспечивающих контакты между людьми, явилось непреодолимое

[1] Исследования аналитической компании Royal Pingdom. Режим доступа: http://quty.ru/news/rezultati-issledovaniya

желание людей общаться между собой в реалиях настоящего времени. Социальные сети – величайший прорыв в истории человечества, популярность которых с каждым днем только нарастает. Взрыв популярности данного проекта, неизбежно, приводит к его глобальному росту. После своего появления социальные сети развивались в основном количественным путем, охватывая все больше пользователей, сегодня же социальные сети переходят в стадию качественного развития, придумывая все новые инструменты взаимодействия с пользователями.

Всего 5-7 лет назад начали активно развиваться социальные сети общего типа: для личного или делового общения; сети, построенные на определенном типе контента; клоны общих сетей для локальных рынков. За общими сетями начали развиваться тематические проекты, которые использовали все тот же механизм социальных сетей, но в конкретной ограниченной нише. Этот процесс начался 3-5 лет назад и сейчас перешел в очень активную стадию. Российские социальные сети развиваются по примеру и опыту соцсетей США и Западной Европы. Небольшие соцсети государств Восточной Европы и СНГ, частично перенимая опыт «старших братьев», параллельно ищут свой путь для достижения наибольшего влияния на своих пользователей.[1]

Социальная сеть – это огромное хранилище данных, которые могут использоваться во многих областях человеческой деятельности, к примеру, в розыскной деятельности сотрудников органов внутренних дел. Ведь, значительное увеличение числа людей занятых информационными технологиями, коммуникациями и ставящих в зависимость от Интернета свое общение и досуг, действительно, предоставляет возможность органам внутренних дел разыскивать скрывшихся подозреваемых, выявлять доказательства совершенных преступлений, а также устанавливать дополнительных участников «темных дел» причастных или

[1] См.: Бондаренко И. Исследование истории и темпов развития социальных сетей в мире. Режим доступа: http://www.timetoast.com/ timelines/социальные-сети-история-развития

непосредственно главенствующих в совершённых преступлениях, анализировать преступную группу и причину преступлений. Так 68 % проанкетированных нами сотрудников указали, что они активно используют Интернет в данных целя (см. прил.1).

Кроме того, следует отметить и тот фактор, что социальные сети в последнее время все активнее используются и в качестве виртуальных площадок для совершения преступлений, связанных с мошенничеством, незаконным оборотом наркотиков, педофилией, терроризмом и экстремистской деятельностью.

Так, социальные сети активно используются для вербовки новых членов террористических организаций, а также в целях массового распространения экстремистской идеологии, что не может не вызывать ужас и опасение за будущие поколения. Как отмечает ОБСЕ, террористические организации превратили дешевые и легкодоступные социальные сети в стратегическое средство для коммуникации, поддержания связей, подстрекательств, восхваления и планирования жесточайших атак на мирное население.[1]

Тем самым, в целях противодействия преступным проявлениям, имеющим отражение в виртуальном мире, а также совершаемых по средствам использования возможностей Интернета, правоохранительным субъектам надлежит иметь представление о социальных сетях, аккумулирующих значительные массивы информации, представляющей интерес в достижении правоохранительных целей.

В самом начале своего развития глобальная паутина предлагала средства коммуникации, позволяющие связывать друг с другом собеседников из разных точек земного шара. Сегодня Всемирная Сеть предлагает еще больше средств, сервисов и услуг, в том числе и

[1] Серия экспертных онлайн-форумов ОБСЕ по использованию Интернета террористами: угрозы, ответы и возможные будущие шаги. Режим доступа: http://www.osce.org/ru/atu/104407?download=true

социальные сети, которые прочно вошли в нашу жизнь и изменили ее.

На данный момент социальные сети, по сути, являются огромной базой данных с самой разнообразной информацией о сотнях миллионов людей по всему миру, которая имеет четкую структуру. В последнее время сети все больше открываются внешнему миру, а многие личные данные пользователей уже доступны для всех желающих. Чем больше человек общается в разнообразных социальных сетях, тем больше информации о нем можно собрать без каких-либо трудов[1]. Именно поэтому открытые источники предоставляют возможность сотрудникам органов внутренних дел получить информацию, имеющую потенциальное доказательственное и оперативно - розыскное значение. Так 64 % опрошенных отметили факт использования информации, имеющейся в базе компаний-владельцев социальных сетей, в своей профессиональной деятельности (см. прил.1).

Современные социальные сети позволяют пользователям указать ряд основных положений (предоставить структурированную по категориям информацию):

- личные анкетные данные;
- фото;
- видео;
- связи (в том числе и по типам);
- интересы;
- образование;
- информацию о работе;
- места, в которых бывает человек;
- предпочитаемые продукты;
- личные мысли и т.д.

Большинство информации, размещаемой в социальных сетях, доступно без регистрации. Достаточно найти страницу пользователя в

[1] См.: Социальные сети. Скрытая угроза для пользователей социальной сети. Режим доступа: http://pro-spo.ru/social/3232-soczialnye-seti-skrytaya-ugroza

популярных социальных сетях, остальное можно увидеть после добавления пользователя в друзья, а вся информация, включая личную переписку (как минимум), доступна администрации этой сети, и никакие настройки приватности не скроют её.[1]

В социальной сети можно найти кого угодно, от школьника до академика, от карманного воришки до члена террористической группировки. В том же «Facebook» зарегистрировано уже около 900 миллионов человек, на сайте «Одноклассники» более 50 миллионов, «ВКонтакте» 56 миллионов и все время продолжают регистрироваться новые участники.

Было бы просто непозволительной глупостью не замечать столь обширные возможности для раскрытия и расследования преступлений, скрывающиеся в «кибернетическом мире» под завесой неграмотности и некомпетентности отдельных сотрудников. Многие могут с уверенностью утверждать, что существует техническая возможность разыскать человека, использующего социальные сети Интернета, но не все знают, как это сделать. Некоторым из опрошенных мешает осуществить данный процесс недостаточно высокий уровень владения компьютером: у 16 % он является средним, позволяющим выполнять базовые операции; 63 % опрошенных имеют лишь общее представление об организации доступа к информационным порталам и о персональном IP-адресе искомых субъектов (см. прил.1). Современный Интернет развивается настолько стремительно, что подключиться к нему может почти каждый, для этого существуют методы и средства, посредством которых пользователи соединяются с Интернетом, пользуясь услугами Интернет-провайдера.

Существует два вида технологий выхода в Интернет:

1. Проводная технология;

2. Беспроводная технология.

---

[1] См.: Социальные сети. Скрытая угроза для пользователей социальной сети. Режим доступа: http://pro-spo.ru/social/3232-soczialnye-seti-skrytaya-ugroza

В каждой из разбираемых технологий присутствуют модемы, которые, в свою очередь, бывают:

1. По исполнению:

- внешние – подключаются через COM, LPT, USB порт или стандартный разъем в сетевой карте RJ-45, обычно имеют отдельный блок питания (существуют и USB-модемы с питанием от шины USB);

- внутренние – дополнительно устанавливаются внутрь аппарата (в слот ISA, PCI, PCI-E, PCMCIA, AMR, CNR);

- встроенные – являются частью аппарата, куда встроены (например, ноутбука или док-станции).

2. По виду соединения:

- модемы для коммутируемых телефонных линий (наиболее распространённый тип модемов);

- ISDN – модемы для цифровых коммутируемых телефонных линий;

- DSL – модемы, применяемые для организации выделенных (некоммутируемых) линий, используя обычную телефонную сеть. Отличаются от коммутируемых модемов тем, что используют другой частотный диапазон, а также тем, что по телефонным линиям сигнал передается только до АТС. Обычно позволяют одновременно с обменом данными осуществлять использование телефонной линии в обычном порядке;

- кабельные – используются для обмена данными по специализированным кабелям, к примеру, через кабель коллективного телевидения по протоколу DOCSIS;

- радио – работают в радиодиапазоне, используют собственные наборы частот и протоколы;

- сотовые – работают по протоколам сотовой связи GPRS, EDGE, и т.п. Часто имеют исполнения в виде USB-брелка. В качестве таких модемов также часто используют терминалы мобильной связи;

- спутниковые – используются для организации спутникового

Интернета (принимают и обрабатывают сигнал, полученный со спутника);

- PLC – используют технологию передачи данных по проводам бытовой электрической сети.[1]

При выборе и использовании одной из перечисленных технологий доступа к сети Интернет, предоставляемых Интернет-провайдером, пользователю автоматически присваивается уникальный IP-адрес, являющийся ничем иным как сетевым адресом абонента (пользователя). Слово «адрес» уже невольно заставляет задуматься, что IP-адрес является своеобразным прототипом «домашнего адреса» человека, по которому к нему всегда можно прийти. Однако, в отличие от «домашнего адреса», IP-адрес представляет собой определенный набор знаков, использование которого в качестве «адреса абонента» обычному обывателю, без знания основных закономерностей его образования, не представляется возможным.

Для разрешения таковой проблемы, следует знать, что IP-адрес может быть как статическим, то есть назначаться только одному непосредственному абоненту (при этом он более не может быть назначен никому другому), так и динамическим – назначаемым одноразово при каждом подключении абонента к сети (каждое новое подключение будет сопровождаться изменением IP-адреса данного абонента).

IP-адрес представляет собой 32-битовое (по версии IPv4) или 128-битовое (по версии IPv6) двоичное число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками, например, 192.168.0.1. IP-адрес состоит из двух частей: номера сети и номера узла.[2] Какая часть адреса относится к

---

[1] Технические средства передачи информации Режим доступа: http://ru.wikiversity.org/wiki/0:%D0%A2%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%81%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%B0_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8

[2] IANA — Number Resources (количество ресурсов). Режим доступа: http://www.iana.org/numbers

номеру сети, а какая к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признаками того, к какому классу относится тот или другой IP-адрес. На рисунке показана структура IP-адреса разных классов.

В случае изолированной сети её адрес может быть выбран администратором из специально зарезервированных для таких сетей блоков адресов (192.168.0.0/16, 172.16.0.0/12 или 10.0.0.0/8). Если же сеть должна работать как составная часть Интернета, то адрес сети выдаётся провайдером либо региональным Интернет-регистратором (Regional Internet Registry, RIR).[1]

Таким образом, чтобы разыскать пользователя того или иного аккаунта в социальной сети, необходимо обладать информацией о его IP-адресе. Искомая информация может быть предоставлена непосредственно владельцами того Интернет-ресурса, которым разыскиваемый абонент пользуется. Здесь следует помнить, что «социальная сеть», это не просто анонимный ресурс в глобальной сети. Владельцем каждого из них выступает та или иная компания.

В свою очередь, сотрудники органов внутренних дел, обладая

[1] См.: Статья: «Что такое IP адрес». Режим доступа: http://2ip.ru/article/ip/?PHPSESSID=mv7hm87rdm8prdvr9f3mmdfr07

простейшими кибернетическими навыками, способны разыскивать, при помощи нескольких методов, скрывшихся подозреваемых, выявлять доказательства совершенных преступлений, а также устанавливать дополнительных участников «темных дел» причастных или непосредственно главенствующих в совершённых преступлениях, анализировать преступную группу и причину преступлений. Ведь IP-адрес не фигурирует в качестве конфиденциальной информации, и соответственно его получение не является нарушением закона ни в российском, ни в каком другом законодательстве стран мира.

Узнать IP-адрес пользователя это не значит узнать фактический адрес проживания, но существует возможность узнать город и страну проживания пользователя, а также получить информацию о его провайдере. В свою очередь провайдер уже имеет данные и о фактическом местоположении пользователя, но без специального официального запроса эти данные не предоставляются, так как считаются личными данными.

Таким образом, одними из методов получения информации об IP-адресе абонента может являться поэтапная процедура запросов управляющим компаниям, услугами которых пользуется разыскиваемый субъект, или использование сотрудниками специальных программ «Снифферов», откладывающих информацию о пользователе того или иного Интернет-ресурса в специальные файлы на сервере (лог сниффера), а именно:

- его IP-адрес;

- время посещения страницы-сниффера;

- адрес страницы, с которой пользователь сделал переход на сниффер.

Юзером в данном случае выступает любой «чатланин» или пользователь CGI скриптов, таких как форум, блог, гостевая книга или социальная сеть (Vkontakte, Odnoklassniki, Facebook, агент Mail.ru, а также ICQ, QIP).

Снифферы – мощное оружие, с помощью которого можно осуществить необходимые оперативные мероприятия. Эта программа может перехватывать и расшифровывать имена и пароли пользователей, конфиденциальную информацию отдельных компьютеров и сети в целом. Известно, что в большинстве протоколов передачи данных (FTP, POP, HTTP, telnet) информация между клиентом и сервером передаётся открытым текстом. Поэтому сотруднику не составит большого труда получить доступ к искомой информации. Достаточно раздобыть программу-сниффер, настроить её фильтры и ждать, когда разыскиваемый субъект будет подключаться к серверу.

Что же касается официального способа получения искомой информации, то следует отметить, что, в соответствии со статьей 38 УПК РФ, следователь является должностным лицом, уполномоченным в пределах своей компетенции осуществлять запросы обязательные для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами. Действуя сообразно ч.4 ст.21 УПК РФ, следователем составляется запрос адресованный руководству компании-владельцу «социальной сети» с просьбой предоставить используемый IP-адрес и время выхода в сеть искомого субъекта. Время выхода в сеть позволит нам индивидуализировать разыскиваемое лицо в случае использования им динамического IP-адреса (см. прил.2).

Обладая информацией об IP-адресе пользователя Интернет-ресурса, полученной одним из перечисленных способов (оперативным либо официальным), должностному лицу предоставляется возможность установить и географическое место выхода абонента в глобальную информационную сеть. Таковыми сведениями, как уже было отмечено, обладает провайдер.

Интернет-провайдер – это оператор связи, имеющий лицензию на один из следующих видов услуг:

- услуги связи по предоставлению каналов связи;

- услуги связи в сети передачи данных, за исключением передачи голосовой информации;

- услуги связи по передаче голосовой информации в сети передачи данных;

- телематические услуги связи.

К примеру, основными провайдерами, действующими на территории Краснодарского края, являются:

- Domashnie Seti Ltd (рейтинг-87.00);

- Noutek Ltd (рейтинг-84.00);

- Linky (рейтинг-74.00);

- SatGate (рейтинг-71.79);

- Link (рейтинг-71.18);

- Сумма Телеком (рейтинг-66.40)[1].

Зная адрес сети, который является составным элементом IP-адреса, следователь может установить Интернет-провайдера искомого субъекта. В этом ему поможет база данных IP-адресов Интернет-провайдеров предоставляемая в открытом доступе на Интернет-ресурсе http://www.2ip.ru.

Формулируя запрос Интернет-провайдеру, информацию о местоположении выхода искомого субъекта возможно получить только при предоставлении ни только полученного IP-адреса, но и времени выхода субъекта в сеть (см. прил.3). В отдельных случаях рекомендуется также предоставлять информацию и о посещаемом искомым субъектом в указываемое время Интернет-ресурсе (в частности конкретной социальной сети). Это позволит индивидуализировать искомого пользователя в случае предоставления Интернет-провайдером услуг связи нескольким пользователям через единый узел связи под идентичным IP-адресом (преимущественно встречается при предоставлении услуг связи в многоквартирные жилые дома и офисы).

[1] Рейтинг провайдеров (г.Краснодар). Режим доступа: http://www.2ip.ru/

Таким образом, знание следователем закономерностей кибернетики, в частности закономерностей организации процесса обмена информацией в сети Интернет, позволяет использовать их в розыске лиц, как скрывающихся от органов предварительного следствия и продолжающих использовать возможности социальных сетей для поддержания связей с привычным им окружением, так и совершающих преступления в кибернетическом пространстве.

Примером тому может служить расследованное уголовное дело, возбужденное в отношении гражданина Б. по факту совершения мошеннических действий, который в процессе расследования скрылся, однако при этом продолжал использовать для общения социальные сети, что позволило установить местонахождения Б. и организовать его задержание[1].

Однако все усилия правоохранительных структур в данной сфере могут быть напрасны в виду того, что в настоящий момент сроки хранения информации о пользователях социальных сетей, а также о передаваемой ими информации через сети Интернет, составляют всего шесть месяцев, что регламентировано ст. 10.1. Федерального закона от 27.07.2006 N149-ФЗ «Об информации, информационных технологиях и о защите информации». Проведенное нами исследование позволяет говорить, что такой срок является недостаточным в виду того, что большинство террористических актов готовятся на протяжении длительного времени и до момента их реализации может пройти не один год, что не позволит при нынешних условиях оперативным подразделениям установить всю цепочку подготовки и совершения преступления. В связи с чем мы считаем, что срок должен быть увеличен до 3 лет, так как 3 года – это достаточный срок для проведения оперативно-розыскных мероприятий, которые позволят воспользоваться столь обширными возможностями по

[1] Уголовное дело №907268, 2011 г. // Архив Прикубанского районного суда г. Краснодара Краснодарского края Российской Федерации.

раскрытию и расследованию преступлений в «кибернетическом мире».

Так же, на наш взгляд, следует значительно расширить и усовершенствовать программное обеспечение в органах внутренних дел, которое беспрепятственно позволит сотрудникам получать искомую информацию в глобальной паутине. Нормативно регламентировать использование разного рода программного обеспечения в поиске и получение оперативно значимой информации в кибернетической сфере компьютерных технологий.

Следует на законодательном уровне определить порядок предоставления доступа к сети Интернет и закрепить в ФЗ от 07.07.2003 N126-ФЗ «О связи» необходимость создания при Министерстве внутренних дел РФ единой межрегиональной базы IP-адресов абонентов с последующим возложением обязанности на Интернет-провайдеров по ее пополнению и поддержанию в ней актуальной информации, которая будет содержать как информацию о провайдере-владельце искомого IP-адреса, так и о владельце оконечного оборудования, которому данный адрес был присвоен.

Кроме того, следует отметить, что оперативные подразделения испытывают затруднения в документировании фактов преступной деятельности в сети Интернет до возбуждения уголовного дела на этапе выявления преступления. Для разрешения сложившейся проблемы, считаем, что надлежит внести изменения в ст. 6 Федерального закона от 12.08.1995 N 144-ФЗ «Об оперативно-розыскной деятельности», дополнив ее новым оперативно-розыскным мероприятием – «осмотр интернет ресурса». Предусмотрев при этом форму закрепления информации в виде акта осмотра интернет ресурса с приложением к нему скриншотов. Данное изменение расширит возможности оперативных подразделений по сбору и закреплению интересующей информации и позволит использовать ее как официальное доказательство.

Подытоживая изложенный в параграфе материал, еще раз следует

отметить ряд основных положений:

1. Информационно-телекоммуникационная система Интернет, в том числе входящие в нее ресурсы социальных сетей, в настоящее время активно используются для в качестве виртуальных площадок для совершения преступлений, связанных с мошенничеством, незаконным оборотом наркотиков, педофилией, терроризмом и экстремистской деятельностью.

2. Ресурсы Интернета в частности, а социальные сети в особенности, могут быть активно, а при должном умении и результативно, использованы в процессе раскрытия и расследования преступлений.

3. Использование Интернет-ресурсов в раскрытии и расследовании преступлений имеет ряд проблем, разрешение которых видится путем внесения изменений и дополнений в ФЗ от 12.08.1995 N 144-ФЗ «Об оперативно-розыскной деятельности», ФЗ от 07.07.2003 N126-ФЗ «О связи» и ФЗ от 27.07.2006 N149-ФЗ «Об информации, информационных технологиях и о защите информации».

2.2. Сотовая связь в раскрытии и расследовании преступлений

Современная сотовая связь представляет собой один из видов радиосвязи, основанный на принципе сотовой сети. Данный принцип заключается в том, что зона обслуживания делится на условные ячейки, так называемые соты, работоспособность которых обеспечивается базовыми станциями связи. Работоспособность такой сотовой сети обеспечивается за счет расположенных на территории приемопередатчиков, работающих в одном диапазоне частот, а также обеспечивающего его коммутирующего оборудования, позволяющего обеспечивать связью передвигающийся в заданной зоне объект. Такая технология на современном этапе развития позволяет оставаться человеку на связи практически в любом индустриальном уголке нашей планеты, что,

безусловно, является одним из двигателей прогресса, обеспечивает возможность увеличить количественную составляющую информационных потоков, реализовать организационные и управленческие задачи.

Зарождение сотовой связи произошло в США в середине XX века. Однако, первыми коммерческими реализациями проекта сотовой связи стали достижения финской сотовой компании «Автомобильный радиотелефон» в 1971 году. Что касается становления коммерческой сотовой связи на территории Российской Федерации, то первые шаги в данном направлении были предприняты в 1990 году, и только к 1997 году эта область телекоммуникации стала активно расширяться.

В настоящее на территории Российской Федерации свою коммерческую деятельность по предоставлению для населения услуг сотовой связи осуществляют такие крупные компании (сотовые операторы), как:

- «МТС» (71 млн. абонентов);
- «МегаФон» (64 млн. абонентов);
- «ВымпелКом» (57 млн. абонентов);
- «Tele2 Россия» (23 млн. абонентов);
- «Ростелеком» (13 млн. абонентов);
- «МОТИВ» (2 млн. абонентов);
- «СМАРТС» (1 млн. абонентов)[1].

На основании представляемых консалтинговым агентством AC&M Consulting данных, доля абонентов сотовых операторов на территории Российской Федерации ежегодно увеличивается в среднем на 8%, при этом несменным лидером в даной области выступает компания «МТС»[2].

---

[1] См.: Список операторов сотовой связи. Свободная энциклопедия Википедия. Режим доступа: http://ru.wikipedia.org/wiki/%D1%EF%E8%F1%EE%EA_%EE%EF%E5%F0%E0%F2%EE%F0%EE%E2_%F1%EE%F2%EE%E2%EE%E9_%F1%E2%FF%E7%E8 (по состоянию на 30 июня 2013 года).

[2] См.: Данные консалтингового агентства AC&M Consulting. Режим доступа: http://www.bit.prime-tass.ru/news/show.asp?id=62789&ct=Telecom

Таким образом, буквально каждый житель нашей страны использует в своей повседневной жизни услуги сотовых операторов. При этом их возможности реализуются как в решении бытовых вопросов, поддержания связи с привычным кругом общения, обеспечения преступной деятельности, так и в реализации профессиональных задач.

Возможности сотовой связи могут быть использованы не только для решения основных, поставленных перед ней задач разработчиками данной системы, то также находят отражение и в правоохранительной сфере. Распространено использование сотовой связи и в преступном мире. При этом таковая может выступать как средством совершения преступления, так и обеспечивающим элементом решения преступных задач. В свете чего, наибольшее значение приобретает, обусловленная технической конструкцией организации сотовой связи, возможность установления местонахождения абонента сотовой системы во время разговора или отправки СМС, а также использования иных услуг передачи данных. Простое, легкое и доступное автоматическое определение местоположения абонента - это не фантастика, а реальность. Еще несколько лет назад подобная возможность могла показаться недостижимой и фантастической.

Наличие мобильного сотового телефона, который можно считать радиомаяком, зачастую позволяет определить как текущее местоположение его владельца, так и проследить его предыдущие перемещения в пространстве.

Каждый абонент использует услуги сотовой связи:

- совершает или принимает звонки;
- отправляет SMS-сообщения;
- пользуется WAP, GPRS услугами.

Информация о действиях абонента сохраняется в виде файла в памяти сервера биллинга. Биллинг — важнейший компонент деятельности любого коммерческого оператора связи, вне зависимости от вида телекоммуникаций: операторы фиксированной и мобильной связи,

Интернет-телефонии, виртуальные операторы, Интернет-провайдеры, операторы транзитного цифрового трафика, провайдеры цифрового телевидения – не могут существовать без биллинга, благодаря которому выставляются счета потребителям их услуг и обеспечивается экономическая составляющая их деятельности. В данном файле содержится следующая информация:

- номер SIM-карты абонента;
- время и продолжительность вызова;
- номер базовой станции (БС);
- номер сектора базовой станции (если имеются сектора) [1].

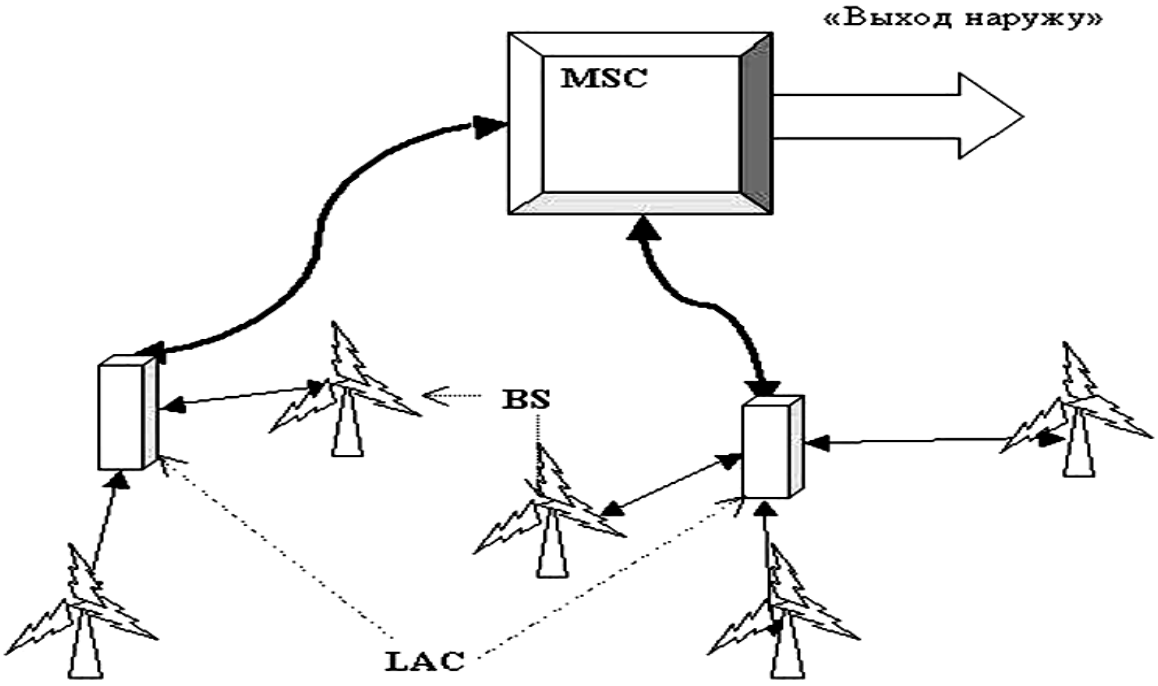
Подробное описание принципа передачи сотового сигнала дают в своем научном труде Мезеря Д.А. и Пахомов С.В. «Когда осуществляется набор номера и происходит вызов абонента, то телефонный аппарат по радиоканалу связывается с одной из антенн ближайшей базовой станции. Каждая из базовых станций содержит от одной до двенадцати приемо-передающих антенн, направленных в разные стороны, чтобы обеспечить связью абонентов со всех сторон. На профессиональном жаргоне антенны также называют «секторами». От антенны сигнал по кабелю передается непосредственно в управляющий блок базовой станции.

Совокупность секторов и управляющего блока обычно и называется – BS, Base Station, базовая станция. Несколько базовых станций, чьи антенны обслуживают какую-либо определенную территорию или район города, подсоединены к специальному блоку – так называемому LAC, Local Area Controller, «контроллер локальной зоны», часто называемому просто контроллером. К одному контроллеру обычно подключается до 15 базовых станций.

В свою очередь, контроллеры, которых также может быть несколько, подключены к самому центральному «мозговому» блоку – MSC,

[1] Бозов А.А. Использование возможностей сотовой связи при раскрытии и расследовании преступлений: Методические рекомендации. 2013. Режим доступа: http://pravorub.ru/personal/30734.html

Mobileservices Switching Center, Центр Управления Мобильными услугами, в простонародье более известный как коммутатор. Коммутатор обеспечивает выход (и вход) на городские телефонные линии, на других операторов сотовой связи и так далее. Схема выглядит примерно так:

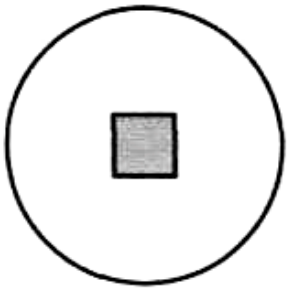


В небольших GSM-сетях используется только один коммутатор, в более крупных, обслуживающих более миллиона абонентов, могут использоваться два, три и более MSC, объединенных между собой. Такая система объединенных центров позволяет осуществлять беспрерывный разговор абонентов во время их перемещений. То есть так называемый «эстафетный принцип» передачи обслуживания в сотовых сетях. Многоуровневая схема сети дает возможность равномерно распределить нагрузку, что снижает вероятность отказа оборудования и, как следствие, потери связи. Если переходить с телефоном из зоны действия одного сектора в зону действия другого, то переводом телефона занимается управляющий блок BS, не затрагивая при этом «вышестоящие» устройства – LAC и MSC. Соответственно, если переход происходит между разными BS, то им управляет LAC и так далее.

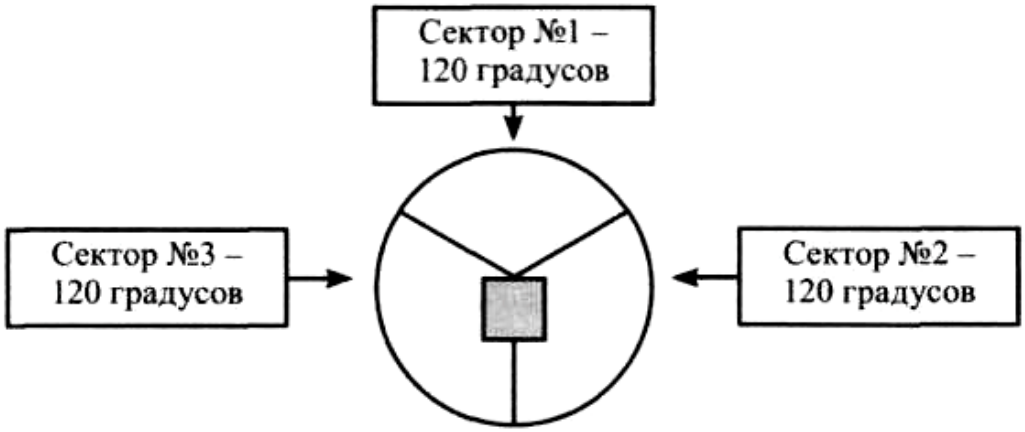
Какая именно базовая станция будет принимать сигнал, определяется специальной компьютерной программой. Она автоматически направляет

соединение на менее загруженную станцию в зоне покрытия, причем это может быть не обязательно ближайшая. Адрес базовой станции определяется по номеру здания, или иного объекта на котором она установлена».[1] Радиус приема сигнала базовых станций зависит от размера зоны действия базовой станции: в лучшем случае погрешность может составлять до 150 метров (пикосота), в худшем — до 30 километров. Данные о том, что соединения приняты конкретной станцией, не означают, что абонент находился рядом именно с данной базовой станцией.

Базовая станция с круговой направленностью



Базовая станция с 3 секторами



Анализ данных в сеансах связи абонента с различными базовыми станциями (через какую и на какую базовую станцию передавался вызов, дата вызова и т.п.) позволяет восстановить все перемещения абонента в прошлом. Такие данные автоматически регистрируются в серверах

[1] Мезеря Д.А., Пахомов С.В. Методика расследования мошенничеств, совершаемых посредством сотовой связи лицами, отбывающими наказание в местах лишения свободы. Учебное пособие. Краснодар, КрУ МВД России. 2014. С. 8-11.

биллинга компаний, предоставляющих услуги сотовой связи, поскольку оплата услуг основана на длительности использования системы.

Этот метод восстановления картины перемещений абонента широко применим в деятельности правоохранительных структур при расследовании уголовных дел, поскольку дает возможность восстановить с высокой временной точностью, где был подозреваемый, с кем встречался (если второй человек также пользовался сотовым телефоном), как долго происходила встреча или был ли подозреваемый поблизости от места преступления в момент его совершения. Так 40 % опрошенных сотрудников в целях раскрытия, расследования и предотвращения преступлений получали информацию о соединениях между абонентами у оператора сотовой связи (см. прил.1).

Например, данный метод был активно использован при расследовании уголовного дела по обвинению граждан С., Б., Г. и Х. в совершении ряда разбойных нападений. Полученные данные биллинга абонентского номера, используемого гражданином С., которому была отведена роль в перевозке членов банды к месту совершения преступления и обратно, позволили доказать причастность данной банды к трем эпизодам разбойных нападений, совершенных на территории Краснодарского края и Республики Адыгея[1].

Как верно отмечает Мезеря Д.А. и Пахомов С.В., «необходимо также понимать, что любой аппарат мобильной связи, а также sim-карта имеют определенный персональный код, который фиксируется операторами сотовой связи при использовании абонентами соответствующих сетей.

На SIM-карте есть специальный номер, так называемый IMSI – International Subscriber Identification Number, Международный познавательный номер абонента. Это номер уникален для каждой SIM-карты в мире, и как раз по нему операторы отличают одного абонента от

[1] Уголовное дело №962881, 2010 г. // Архив Северского районного суда Краснодарского края Российской Федерации.

другого. При включении телефона он посылает этот код, базовая станция передает его на LAC, а LAC, в свою очередь, на коммутатор. Тут в действие вступают два дополнительных модуля, связанных с коммутатором – HLR (Home Location Register) и VLR (Visitor Location Register). Соответственно, Регистр Домашних Абонентов и Регистр Гостевых Абонентов.

В HLR хранятся IMSI всех абонентов, которые подключены к данному оператору. В VLR в свою очередь содержатся данные обо всех абонентах, которые в данный момент пользуются сетью данного оператора. IMSI передается в HLR (в зашифрованном виде). HLR, в свою очередь, проверяет – есть ли у него такой абонент, и, если есть, то не заблокирован ли он, например, за неуплату. Если все в порядке, то этот абонент прописывается в VLR и с этого момента может совершать звонки. У крупных операторов может быть не один, а несколько параллельно работающих HLR и VLR.

Мобильное устройство (телефон, смартфон и др.) стандарта GSM имеет свой индивидуальный номер, состоящий из 15 цифр - IMEI (International Mobile Equipment Identifier, Международный Идентификатор Мобильного Оборудования). Любой владелец данного устройства может посмотреть IMEI своего телефона, набрав на клавиатуре *#06# . Номер IMEI также прописан на коробке устройства и в его гарантийном талоне. При включении телефона и присоединении последнего к сети оператора связи, телефон передает свой IMEI в качестве некоей личной подписи. Оператор связи обычно регистрирует в своих электронных записях, когда и с какой SIM-картой данный телефон подключился к сети.

Все последующие действия, связанные с использованием sim-карт с другим телефоном, или телефона с другой sim-картой, учитываются

оператором сотовой связи. При этом становится возможным проследить «историю» указанных манипуляций». [1]

SIM – это стандартный модуль подлинности абонента, представляющий собой чип, в котором прошит международный идентификационный номер – IMSI, свой индивидуальный ключ аутентификации – К и алгоритм аутентификации. В SIM-карте имеется память для записной книжки, рассчитанная на 100 и более абонентов. Для обеспечения защитных функций SIM-карте присваиваются определенные коды. С помощью записанной в SIM-карте информации, в результате взаимного обмена данными между подвижной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети. Процедура проверки реализуется следующим образом: сеть передает номер на подвижную станцию, в SIM-карте производится вычисление ответа, который передается в сеть и сравнивается с правильным решением, формируемым в специальном модуле подсистемы коммутации – центре аутентификации.

Имеется техническая возможность определить текущее положение абонента и перемещение абонента в прошлом. Текущее положение может выявляться двумя способами. Первым из них является метод триангуляции (пеленгования) из трех точек. Второй способ — через компьютер компании, предоставляющей связь, который постоянно регистрирует, где находится тот или иной абонент в данный момент времени даже в том случае, если он не ведет разговоров (по идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию). Точность определения местоположения абонента в этом случае зависит от целого ряда факторов: пересеченности местности, наличия помех и переотражений от зданий, положения базовых станций, количества работающих в настоящий момент телефонов в данной соте. Большое

[1] Мезеря Д.А., Пахомов С.В. Методика расследования мошенничеств, совершаемых посредством сотовой связи лицами, отбывающими наказание в местах лишения свободы. Учебное пособие. Краснодар, КрУ МВД России. 2014. С. 11-12.

значение имеет и размер соты, в которой находится абонент, поэтому точность определения места его нахождения в городе гораздо выше, чем в сельской местности.

Анализ данных о сеансах связи абонента с различными базовыми станциями позволяет восстановить все перемещения абонента в прошлом. Такие данные автоматически регистрируются в компьютерах компаний, поскольку оплата их услуг основана на длительном использовании системы связи. В зависимости от вида оператора связи подобная информация хранится от 60 дней до 7 лет.

Существует ряд технологий определения местоположения абонента применительно к стандарту GSM:

1. Позиционирование по Cell Id. Это самая простая технология определения примерного положения абонента по идентификатору соты (Cell Identifi), основанная на том, что в момент локализации или ведения разговора мобильная станция связывается с сетью и обменивается служебной информацией;

2. Позиционирование по времени прибытия. Такая технология основана на анализе измерения промежутка времени, за который сигнал с мобильной станции достигает как минимум трех базовых станций, оснащенных блоками определения местоположения. При этом специальный компьютер собирает полученную информацию и рассчитывает местоположение абонента методом триангуляции (пеленгования).

Данный метод дает высокие показатели, но из-за дороговизны, увеличения нагрузки сети не нашел широкого применения;

3. Позиционирование с помощью системы GPS. Технология основана на использовании спутниковой системы позиционирования GPS и дает точность определения места нахождения абонента до 10 метров на открытой местности и до десятков метров в помещении с окнами. Точность определения снижается, если аппаратура «не видит» четырех

спутников. Для использования этой технологии необходимо оборудование мобильного приемника GPS-приемником;

4. Позиционирование с помощью разницы во времени. Технология во многом подобна позиционированию по времени прибытия. Мобильная станция играет более активную роль, измеряя время прохождения сигнала до нее от одной базовой станции, оснащенной специальным блоком, и сравнивает его с соответствующим временем прохождения сигнала не менее, чем от еще двух станций. Расстояние между базовыми блоками известно и известно время прохождения сигналов от каждого из них. С мобильного телефона информация передается в сеть на специальный компьютер, который производит соответствующие вычисления[1].

Таким образом, проводимый в коммерческих целях биллинг пользователей сотовой связи, может представлять собой потенциальную доказательственную базу по широкому перечню преступных деяний, позволяющую принять правоохранительным структурам при их расследовании обоснованное и объективное решение.

Так, при расследовании того или иного уголовного дела, сотруднику правоохранительных органов для получения биллинга соединений достаточно обладать любыми одними из следующего ряда сведений данными:

- о проверяемом лице (анкетные данные субъекта, использовавшего сотовый телефон);

- об IMEI-номере телефона, использованного для переговоров или совершения преступления;

- об абонентском номере;

- о номере SIM-карты.

[1] См.: Базов А.А. Использование возможностей сотовой связи при раскрытии и расследовании преступлений: Методические рекомендации. 2013. Режим доступа: http://pravorub.ru/personal/30734.html

Наличие указанных сведений позволит следователю составить запрос тому или иному оператору сотовой связи и получить недостающие ему сведения, необходимые для составления постановления о возбуждении перед судом ходатайства о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами (см. прил.4, прил.5).

Более того, даже не обладая соответствующей информацией, использование возможностей биллинга не исчерпывается. Так, следователь может получить у операторов сотовой связи информацию о произведенных соединениях по обмену информацией через каналы сотовой связи за определенный промежуток времени на определенной территории (например, в за пол часа до и после совершения преступления в пределах 0,5 км. от места убийства). Данная информация также может иметь значение для установления субъекта, совершившего преступление, вероятно, пользовавшегося услугами сотовых операторов.

Однако, в недавнем времени были приняты ряд изменений в действующее законодательство Российской Федерации, создающие для правоохранительных органов трудности в процессе получения оговоренных сведений:

- Федеральный закон Российской Федерации от 25 декабря 2012 г. №253-ФЗ «О внесении изменений в Федеральный закон «О связи» и статьи 333.33 и 333.34 части второй Налогового кодекса Российской Федерации»;

- Постановление Правительства РФ от 15 июля 2013 г. №599 «О внесении изменений в Правила оказания услуг подвижной связи»;

- Постановление Правительства Российской Федерации от 28 ноября 2013 г. №1094 «О внесении изменений в постановление Правительства Российской Федерации от 15 июля 2013 г. №599»;

- Федеральный закон от 25.11.2013 №314-ФЗ «О внесении изменения в статью 46 Федерального закона «О связи».

Изменения, в первую очередь, позволяют абонентам той или иной сотовой сети изменять сотового оператора без изменений своего

абонентского номера. Такой порядок может создать затруднения в определении принадлежности абонентского номера конкретной сотовой сети, так как единого открытого ресурса переноса абонентских номеров в настоящее время не разработано. В свете чего, при составлении запросов сотовым операторам, (см. прил.4) таковые сведения в настоящее время также следует уточнять. Данный факт может в значительной степени затянуть определение оператора связи и, тем самым, затруднить получение оговоренных сведений.

Однако, как мы считаем, преодолеть отмеченные трудности, облегчить и оптимизировать деятельность правоохранительных структур в данной сфере, позволит создание единого ресурса переноса абонентских номеров от одного оператора сотовой связи к другому.

Подытоживая изложенную в рамках данного параграфа информацию, следует отметить ряд основных положений:

1. Кибернетические закономерности организации обмена информацией в сфере сотовой телекоммуникации могут быть использованы сотрудниками правоохранительных подразделений для определения местоположения субъекта, использующего услуги сотовых операторов, что применимо для разрешения ряда вопросов в процессе раскрытия и расследования преступлений.

2. Современные законодательные тенденции в сфере сотовой телекоммуникации несут благие улучшения для борьбы с монополизацией рынка сотовых услуг связи, но в то же время имеют пробелы, требующие разрешения. Видится целесообразным создание единой базы данных в правоохранительной структуре, отражающей принадлежность того или иного абонентского номера определенному сотовому оператору и информацию о владельце такового.

2.3. Электронная почтовая связь, как безмолвный свидетель

Современный мир – продукт длительного предшествующего развития, благодаря техническому прогрессу мы знаем то, чего не знали ранее. Всего несколько лет назад фраза «виртуальная реальность» обозначала что-то, что казалось всем безобидной игрушкой или даже приятным развлечением. Сейчас значительная доля населения Земли столь плотно вовлечена в эту иную реальность, что буквально не мыслит без нее ни труда, ни общения. Живое, реальное общение вытеснили смайлы и набор буквенных символов. Большинство из нас уже забыли, как писать бумажные письма, как выражать чувства на бумаге. Мы предпочитаем звонить, ведь это гораздо проще и быстрее, писать электронные письма с двумя-тремя предложениями информационного характера. Такое общение занимает мало времени, но ставит в глубокую зависимость от компаний, предоставляющих данные услуги, ведь они без труда могут проследить каждый наш шаг.

Электронная почта является одним из древнейших сервисов Интернета, который используется для передачи информации и виртуального общения в компьютерных сетях. Электронная почта (e-mail) - это совокупность средств, предназначенных для обмена сообщениями между пользователями компьютерной сети.

Электронная почта является самым популярным сервисом Интернета, что связано с ее существенными преимуществами по сравнению с обычной «бумажной» почтой:

- электронные сообщения передаются с огромной скоростью (на это уходит несколько секунд);

- в электронном письме можно передать не только тексты, но и мультимедийные данные (любые изображения, аудио - или видеозапись) и другие файлы;

- пользователь может не сразу отвечать на электронное письмо, есть время обдумать собственный ответ и принять взвешенное решение;

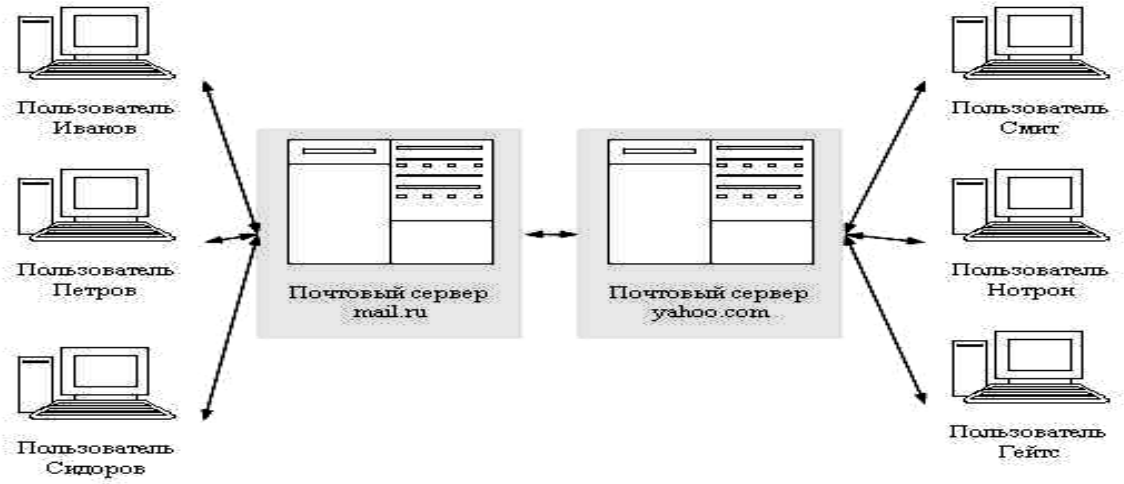
- стоимость электронного письма гораздо меньше стоимости обычного «бумажного», поскольку не нужно тратить средства на приобретение бумаги, конверта, марок или оплачивать услуги почты по доставке этого письма;

- электронное письмо можно одновременно отправить всей группе получателей, перенаправить на другой адрес электронной почты;

- обрабатывая сообщения, полученные по электронной почте, можно использовать услуги автоответчика, назначив автоматически создавать ответы на полученные письма;

- создать определенные правила и использовать их при электронной переписке, назначив выполнять одинаковые действия с электронными уведомлениями одного типа (например, назначить автоматически удалять электронные письма рекламного характера или письма, поступающие с определенного адреса).

Принцип работы электронной почты довольно прост: подключаемся к компьютерной системе, пишем письмо и отправляем его человеку, чей компьютер подключен к другой системе. Сообщение идет по лабиринту связанных между собой компьютерных систем, пока не дойдет до места назначения. То есть пользователь в режиме off-line пишет текст письма, указывает адрес получателя. Для этого используется редактор подготовки писем, входящий в клиент-программу электронной почты. Подготовленные письма помещаются в папку «Исходящие». Затем устанавливается связь с сервером. Далее происходит автоматическая работа в режиме on-line: сервер по паролю определяет пользователя, принимает все письма из папки «Исходящие», передаёт поступившие письма, которые помещаются в папку «Входящие». Сеанс связи закончен. Папка «Исходящие» стала пустой, отправленные письма сохранились в папке «Отправленные». Если используется коммутируемая телефонная линия, то пользователь отключает телефонную связь. После этого он может не спеша просматривать полученную почту.



Почтовый сервер работает постоянно. Он периодически просматривает «почтовые ящики» и организует передачу по сети исходящих писем. Входящую корреспонденцию почтовый сервер раскладывает по «ящикам».

Рассматривая принцип работы электронной почты, нельзя не дать определения основным понятиям: SMTP, POP3, MDA, MUA, MTA.

- SMTP (Simple Mail Transfer Protocol) – протокол применяется для пересылки почтовых сообщений как между клиентом и сервером, так и между серверами.

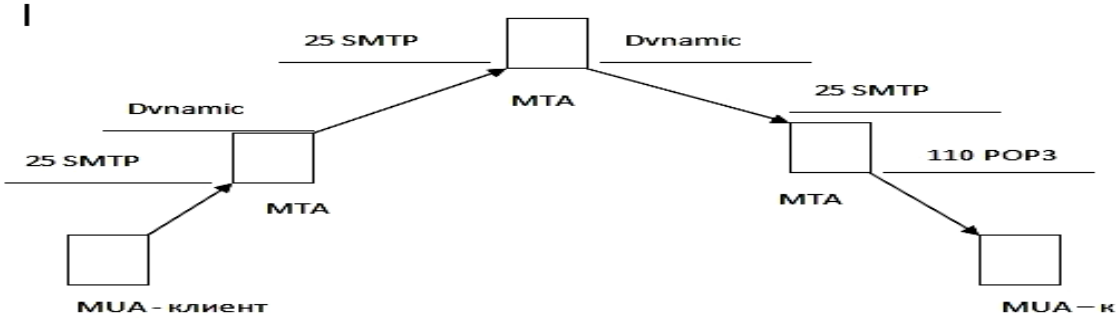
- POP3 (Post Office Protocol v3) – протокол, применяемый для управления почтовым сервером и получения сообщений от сервера клиенту.

- MUA (Mail User Agent) – приложение пользователя, выполняющее пересылку почтового сообщения на сервер, указанный в настройках приложения.

- MTA (Mail Transfer Agent) – почтовый сервер, выполняющий хранение и пересылку сообщений.

- MDA (Mail Delivery Agent) – приложение, забирающее почту пользователя с других серверов и хранящее или пересылающее их определенному пользователю. К примеру, есть несколько аккаунтов электронной почты. MDA заходит на все сервера и перенаправляет все

письма посредством почтовых серверов, на которые заходит программа на один определенный адрес.[1]



Сообщение в электронной почте состоит из заголовка и тела. Заголовок обычно включает:

- уникальный идентификационный номер сообщения;

- адрес отправителя сообщения;

- адрес получателя сообщения (получателей может быть несколько);

- тему сообщения;

- время и дату отправления сообщения.

В заголовок может вставляться информация о маршруте – узлах сети, через которые будет передано сообщение.

Системы электронной почты предоставляют пользователям следующие основные возможности:

- оповещение о прибытии почты;

- наличие встроенного текстового редактора;

- наличие нескольких вариантов адресации сообщений;

- присоединение файлов – посылка файла вместе с сообщением;

- чтение почты;

- обработка сообщений;

- хранение сообщений. Многие системы позволяют распределить сообщения по папкам в соответствии с их тематикой. Системы электронной почты с расширенными возможностями позволяют хранить

[1] См.: Принцип работы электронной почты - E-Mail. Режим доступа: http://it-student.com.ua/servisy-i-slujby/main/princip-raboty-elektronnoi-pochty-e-mail.html

связанные сообщения – последовательность сообщений запоминается в формате, имитирующем диалог;

- наличие списков рассылки – хранение наборов имен, объединенных под одним заголовком и рассматриваемых как один адрес электронной почты;

- наличие форм – средств отображения структурированной информации;

- распределение полномочий – разрешение или запрещение доступа к личному почтовому ящику;

- обеспечение безопасности – введение пароля, шифрование информации;[1]

- предоставление сведений об IP-адресе отправителя электронного почтового сообщения.

Современный почтовый ящик, к примеру, компании «mail.ru», представляет собой каталог, состоящий из следующих элементов:

- входящие, отправленные и непрочитанные письма;

- адресная книга, как средство для работы с адресами электронной почты. Это средство управления базой данных, обычно встроенное в почтовую программу, которое позволяет вести учет контактов;

- белый список почтовых адресов, список адресов электронной почты, который используют, чтобы пропускать избранные сообщения в тех случаях, когда почтовый клиент настроен на блокирование всех поступающих сообщений;

- черный список почтовых адресов, список адресов электронной почты, сообщения от которых автоматически блокируются и уничтожаются непосредственно на сервере без загрузки на локальный компьютер;

[1] См.: Электронная почта. Основные возможности. Структура почтового сообщения. Программные средства. Режим доступа: http://www.yaklass.ru/materiali?mode=cht&chtid=465

- контакт, запись адресной книги, соответствующая регулярным корреспондентам и содержащие данные о людях и их адресах электронной почты;

- корзина, для удаления не востребованных входящих и исходящих писем.

Субъекты преступлений, особенно реализующие свою противоправную деятельность в сети Интернет, как и другие пользователи, вынуждены использовать электронные почтовые ресурсы как в качестве средства передачи информации, так и в качестве обязательного требования для регистрации и пользования сторонними Интернет-ресурсами, требующими процедуры аутентификации.

Данные обстоятельства позволяют говорить об использовании возможностей электронных почтовых ресурсов в двух направлениях:

1) Для получения информации, касающейся преступного проявления;

2) Для минимизации случаев анонимного использования ресурсов Интернета, в том числе субъектами преступлений, реализующих свою противоправную деятельность при помощи обозначенных телекоммуникационных систем.

В рамках первого направления электронная почтовая переписка субъектов преступления может представлять интерес для правоохранительных органов в двух направлениях:

1. В целях использования сведений об IP-адресе пользователя почтового аккаунта для установления его местонахождения.

2. В целях получения доказательственной информации, представляющей значение для процесса раскрытия и расследования преступления, содержащейся в переписке пользователя почтового аккаунта.

Что касается установление местонахождения по сведениям об IP-адресе, то его использование строится по аналогии изложенному в первом

параграфе второй главы данного учебного пособия, в котором мы подробно рассматривали возможность поиска субъектов в кибернетическом пространстве, описывали методы, способы и алгоритм действий для осуществления поиска и получения необходимой информации. Алгоритм действий для поиска скрывшихся подозреваемых и получения доказательств совершенных преступлений при использовании возможностей электронной почты не изменился.

В свою очередь сама информация, содержащаяся в письмах, хранимых на сервере электронной почты, может иметь потенциальное доказательственное и оперативно-розыскное значение. Так 60 % опрошенных сотрудников подтверждают, что при расследовании уголовных дел осуществляли изъятие таковой информации. В тоже время 40 % опрошенных указало, что испытывают затруднения или вовсе не обладают информацией о процессе получения таковых сведений из электронных почтовых ресурсов (см. прил.1).

Владелец почтового аккаунта мог вести активную переписку с иными участниками «темного» дела, передавать разного рода и степени важности документы для заключения сделок, отправлять аудио и видео файлы с места преступления, переговоров и файлы несущие разного рода смысловую нагрузку.

В целях получения таковой информации, следователь может использовать ряд предоставленных ему полномочий. Он, в пределах своей компетенции, с согласия руководителя следственного органа, возбуждает ходатайство перед судом о производстве выемки почтовой корреспонденции с электронного ресурса в соответствие со ст. 38, частью первой ст. 165, частями первой, второй и четвёртой ст. 182 и ст. 183 УПК РФ (см. прил.6).

В результате проведения выемки данной электронной информации следователем будет получено следующее:

1. Регистрационные данные абонента почтового ресурса;

2. Электронный носитель с базой данных почтового ресурса, на котором происходила выемка электронной почтовой корреспонденции.

Полученные данные, изъятые следователем в ходе выемки на почтовом ресурсе, в порядке ст.164, ч.1 ст.176, ч.1-4 и 6 ст.177 УПК РФ следует осмотреть в целях обнаружения следов преступления и выяснения обстоятельств, имеющих значение для раскрытия и расследования преступления.

При этом информация, полученная при проведении выемки с почтового ресурса, предоставленная следователю на электронном носителе, может быть (в зависимости от почтового компании) представлена в закодированном виде. Данный факт может представлять собой непреодолимое неудобство для лиц несведущих в конвертировании файлов из одного расширения в другое и не позволить произвести качественный осмотр полученной электронной информации.

Так, при расследовании уголовного дела была произведена выемка электронной информации с почтового ресурса ООО «МЕЙЛ.РУ». В ходе осмотра полученной информации установлено, что вся электронная переписка гражданина А. предоставлена в файлах разрешением «base64», не читаемых стандартным программным обеспечением Windows XP. В целях получения доказательственной информации, данные файлы были конвертированы в расширение «eml», что позволило их просмотр и изучение содержимого при помощи использования почтовой утилиты Outlook Express. Результаты осмотра электронной почтовой корреспонденции оказали существенной значение для процесса расследования данного уголовного дела[1].

Таким образом, следователю, как минимум, для проведения осмотра таких сведений, необходимо обладать навыками использования программных почтовых утилитов, например Outlook Express.

[1] Уголовное дело № 962270, 2010 г. // Архив Северского районного суда Краснодарского края Российской Федерации.

Говоря о втором направлении использования почтовых ресурсов, следует отметить, что, не смотря на возможное существенное значение для раскрытия и расследования преступлений данных из электронных почтовых ресурсов, при прохождении регистрации для получения почтового ящика пользователь, вводя свои персональные данные (идентификационные данные), к сожалению, может ввести любые сведения, даже не принадлежащие ему. Это в значительной степень может затруднить действия по установлению принадлежности конкретного почтового аккаунта тому или иному реальному субъекту нашего общества.

В свете чего, так как почтовый аккаунт (электронный почтовый ящик) в настоящее время выступает в рамках глобальной информационной сети Интернет чуть ли не основным идентификатором при регистрации на любых ресурсах Интернета, видится целесообразным узаконить процедуру регистрации данных почтовых аккаунтов. На основании чего, мы считаем необходимым при прохождении регистрации и заполнении индивидуальных данных ввести привязку к паспортным данным граждан, изъявляющих желание на получение доступа к электронному почтовому ресурсу. В качестве единого портала, обеспечивающего соблюдение таких требований, предлагается использовать единый «Портал государственных услуг» (http://www.gosuslugi.ru/), выступающий гарантом предоставления данных о личности.

Такая система действительно поможем индивидуализировать лицо, ведь паспортные данные уникальны и единичны. Более того, ряд почтовых компаний в сети Интернет уже давно используют паспортные данные в качестве вспомогательного средства при восстановлении доступа законному владельцу при взломе почтового аккаунта злоумышленниками. Предложенные меры позволят сделать Интернет-среду более прозрачной и менее анонимной, что, как мы считаем, уменьшит случаи анонимного использования возможностей современных информационно-телекоммуникационных систем в преступных целях.

Подытоживая изложенную информацию в рамках данного параграфа, следует отметить следующие важные положения:

1. Электронные почтовые ресурсы активно используются всеми пользователями сети Интернет и являются основным идентификатором личности субъекта в информационном поле Интернета;

2. Использование преступными элементами возможностей электронных почтовых ресурсов позволяет определить их фактическое местонахождение, а также получить информацию, потенциально имеющую доказательственное значение для раскрытия и расследования преступления;

3. Имеется целесообразность нормативно-правового закрепления порядка регистрации пользователей в электронных почтовых системах с использованием их индивидуальных паспортных данных, что позволит сделать Интернет-среду менее анонимной и более безопасной.

ЗАКЛЮЧЕНИЕ

XXI век – это время глобальных изменений, охватывающих все сферы жизни человека: политику, экономику, образование, культуру и, конечно же, науку. Именно прогресс, проявляющийся в науке в совершенствовании методов, позволяет решать поставленные задачи и разрешать злободневные проблемы по раскрытию, расследованию и предупреждению преступлений сотрудниками органов внутренних дел.

Век высоких информационных технологий диктует моду на Интернет и поставил в зависимость от глобальной компьютерной сети уже более 2,4 млрд. людей. Нынешнее подчиненное положение людей от Интернета предоставляет возможным сотрудникам органов внутренних дел проводить различные следственные действия в кибернетическом пространстве.

На основании развития научной деятельности, расширяющей возможности сотрудников органов внутренних дел в розыске лиц в глобальной паутине, нами были рассмотрены основные возможности такого розыска и выполнены основные задачи, поставленные нами при написании данного учебного пособия. Мы выявили основные методы по розыску скрывшихся подозреваемых, выявлению доказательств совершенных преступлений в социальных сетях, поиску субъектов при помощи сотовых операторов связи и получению оперативной информации с безмолвного свидетеля - электронной почты Интернета.

В учебном пособии разрешены следующие основные задачи:

- дано понятие и характеристика кибернетики как науки;

- раскрыто понятие «кибернетика», как один из источников криминалистики;

- исследована возможность и необходимость использования современных достижений науки и техники, информационных систем, сетей связи, а также современных информационно-телекоммуникационных

инфраструктур в профессиональной деятельности сотрудников органов внутренних дел;

- исследована реализация разного рода служебных задач при помощи знания законов кибернетики (законов информационных потоков).

На основании теоретической основы исследования и эмпирических источников в представленном учебном пособии сделаны следующие выводы и вынесены предложения по совершенствованию как организационных моментов раскрытия и расследования преступлений, так и законодательной базы:

1. В настоящее время не существует единого понимания кибернетики. Не смотря на это, в течение времени она смогла сформироваться в отдельную науку со своими задачами, законами и принципами, имеющими разветвленные направления в различных областях знаний биологии, математики, медицины, информатики, психологии, физики, химии и других наук, объединенных при исследовании управления системами.

2. Кибернетика как источник криминалистики, оказывает влияние на криминалистику в двух сферах:

- использование достижений кибернетики позволяет оптимизировать криминалистику как управляемую структуру, а именно саму организацию процесса по выявлению, раскрытию и расследованию преступлений;

- использование знаний о принципах передачи, хранения и переработки информации в системах, позволяет сформировать представление об организации процесса получения криминалистически значимой информации из данных систем (к таковым могут быть отнесены информационно-телекоммуникационная система Интернет, социальные сети и электронные почтовые ресурсы как составные элементы Интернета, система сотовой связи и т.п.).

3. Социальные сети в современном обществе играют значимую роль и могут быть активно, а при должном умении и результативно,

использованы в процессе раскрытия и расследования преступлений:

- в целях установления местонахождения скрывшегося субъекта, продолжающего использовать возможности социальных сетей;

- для получения информации о круге общения, интересах, увлечениях, навыках отдельного субъекта;

- для выявления доказательств совершенных преступлений и установления дополнительных участников «темных дел» причастных или непосредственно главенствующих в совершённых преступлениях;

- при анализировании преступной группы и причин преступлений;

- в целях получения иных сведений, представляющих значение для раскрытия и расследования преступлений.

4. Имеется необходимость создания при Министерстве внутренних дел РФ единой межрегиональной базы IP-адресов абонентов с последующим возложением обязанности на Интернет-провайдеров по ее пополнению и поддержанию в ней актуальной информации.

5. Видится потребность в увеличении сроков хранения информации в сети «Интернет» и информацию о пользователях данной сети, регламентированных ст. 10.1. Федерального закона от 27.07.2006 N149-ФЗ, с шести месяцев до трех лет. Это позволит при нынешних условиях оперативным подразделениям установить всю цепочку подготовки и совершения террористических и экстремистских преступлений.

6. Назрела необходимость внести изменения в ст. 6 Федерального закона от 12.08.1995 N 144-ФЗ "Об оперативно-розыскной деятельности", дополнив ее новым оперативно-розыскным мероприятием – «осмотр интернет ресурса», предусмотрев при этом форму закрепления информации в виде акта осмотра интернет ресурса с приложением к нему скриншотов. Данное изменение расширит возможности оперативных подразделений по сбору и закреплению соответствующей информации и позволит использовать ее как официальное доказательство.

7. Кибернетические закономерности организации обмена

информацией в сфере сотовой телекоммуникации могут быть использованы сотрудниками правоохранительных подразделений для определения местоположения субъекта, использующего услуги сотовых операторов, что применимо для разрешения ряда вопросов в процессе раскрытия и расследования преступлений:

- установления местонахождения интересуемого субъекта до, во время и после совершенного преступления;

- установления маршрута передвижения интересуемого субъекта в определенный промежуток времени;

- установления связей отдельного субъекта с другими лицами и т.д.

8. Современные законодательные тенденции в сфере сотовой телекоммуникации несут благие улучшения для борьбы с монополизацией рынка сотовых услуг связи, но в то же время имеют пробелы, требующие разрешения. Видится целесообразным создание единой базы данных в правоохранительной структуре, отражающей принадлежность того или иного абонентского номера определенному сотовому оператору и информацию о владельце такового.

8. Электронные почтовые ресурсы активно используются всеми пользователями сети Интернет и являются основным идентификатором личности субъекта в информационном поле Интернета;

9. Использование субъектом преступления электронных почтовых ресурсов представляет возможность правоохранительным структурам определить его фактическое местонахождение, а также получить информацию, потенциально имеющую доказательственное значение для раскрытия и расследования преступления:

- о личности ведущих переписку;

- о сведениях получаемых и сообщаемых (передаваемых) по каналам электронной почтовой связи интересующим субъектом и т.п.

10. Имеется целесообразность нормативно-правового закрепления порядка регистрации пользователей в электронных почтовых системах с

использованием их индивидуальных паспортных данных. В качестве единого портала, обеспечивающего соблюдение таких требований, предлагается использовать единый «Портал государственных услуг» (http://www.gosuslugi.ru/), выступающий гарантом предоставления данных о личности. Данное решение уменьшит анонимность и позволит сделать Интернет-среду более безопасной от преступных проявлений.

Таким образом, в условиях, характеризующихся значительным увеличение числа людей, занятых информационными технологиями, коммуникациями и ставящих в зависимость от интернета свое общение и досуг, действительно предоставляется возможность органам внутренних дел разыскивать скрывшихся подозреваемых и интересующих следствие субъектов, выявлять доказательства совершенных преступлений, а также устанавливать дополнительных участников «темных дел», причастных или непосредственно главенствующих в совершённых преступлениях, анализировать преступную группу и причину преступлений. Ведь Интернет - это глобальная компьютерная сеть, охватывающая весь мир. В последние годы Интернет претерпевает большой подъем как в мире, так и в нашей стране. Он является самым быстрым и доступным поставщиком информации и связи между людьми на расстоянии многих тысяч километров.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Нормативные правовые акты:

1. Конституция Российской Федерации (ред. от 30 дек. 2008 г.) // Российская газета. – 2009. – № 7. – 21 янв.

2. Уголовный Кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. (ред. от 19 апр. 2013 г.) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

3. Уголовно - процессуальный Кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 21 янв. 2014 г.) // Собрание законодательства РФ. – 2001. - № 52 (ч.1). – Ст. 4921.

4. О полиции: федеральный закон Российской Федерации № 3-ФЗ от 7 февр. 2011 г. (ред. от 5 апр. 2013 г.) // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

5. Об оперативно-розыскной деятельности: федеральный закон Российской Федерации № 144-ФЗ от 12 августа 2005 г. (ред. от 5 апр. 2013 г.) // Собрание законодательства РФ. –1999. – № 33. – Ст. 3349.

6. О связи: федеральный закон Российской Федерации № 126-ФЗ от 07 июля 2003 г. (ред. от 28 дек. 2013 г.) // Собрание законодательства РФ. – 2003. – № 28. – Ст. 2895.

7. Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации № 149-ФЗ от 27 июля 2006 г. (ред. от 28 декабря 2013 г. с изм. и доп., вступ. в силу с 01 февраля 2014 г.) // Собрание законодательства РФ. – 2006. – № 31 (ч.1). – Ст. 3448.

8. О внесении изменений в Федеральный закон «О связи» и статьи 333.33 и 333.34 части второй Налогового кодекса Российской Федерации: федеральный закон Российской Федерации № 253-ФЗ от 25 декабря 2012 г. // Собрание законодательства РФ. – 2012. – № 53 (ч.1). – Ст. 7578.

9. О внесении изменения в статью 46 Федерального закона «О

связи»: федеральный закон Российской Федерации № 314-ФЗ от 25 ноября 2013 г. // Собрание законодательства РФ. – 2013. – № 48. – Ст. 6162.

10. О внесении изменений в Правила оказания услуг подвижной связи: постановление Правительства РФ № 599 от 15 июля 2013 г. (ред. от 28 ноября 2013 г.) // Собрание законодательства РФ. – 2013. – № 29. – Ст. 3975.

11. О внесении изменений в постановление Правительства Российской Федерации от 15 июля 2013 г. № 599: постановление Правительства РФ № 1094 от 28 ноября 2013 г. // Собрание законодательства РФ. – 2013. – № 48. – Ст. 6280.

12. О структуре федеральных органов исполнительной власти: указ Президента РФ № 636 от 21 мая 2012 г. (ред. от 01 ноября 2013 г.) // Собрание законодательства РФ. – 2012. – № 22. – Ст. 2754.

13. Вопросы Министерства внутренних дел Российской Федерации: указ Президента РФ № 248 от 1 марта 2011 г. (ред. от 25 декабря 2013 г.) // Собрание законодательства РФ. – 2011. – № 10. – Ст. 1334.

2. Судебная и следственная практика:

1. Уголовное дело №907268, 2011 г. // Архив Прикубанского районного суда г. Краснодара Краснодарского края Российской Федерации.

2. Уголовное дело №962881, 2010 г. // Архив Северского районного суда Краснодарского края Российской Федерации.

3. Уголовное дело № 962270, 2010 г. // Архив Северского районного суда Краснодарского края Российской Федерации.

3. Научная и научно-практическая литература:

1. Абдеев Р.Ф. Философия информационной цивилизации / Р.Ф. Абдеев. – М.: ВЛАДОС, 1994. – 336 с.

2. Белкин Р.С. Криминалистика: проблемы, тенденции,

перспективы. Общая и частные теории / Р.С. Белкин. – М.: Юридическая литература, 1987. – 272 с.

3. Винер Н. Кибернетика, или управление и связь в животном и машине / Н. Винер. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – 344 с.

4. Винер Н. Кибернетика и общество / Н. Винер. – М.: Издательство иностранной литературы, 1958. – 200 с.

5. Гончарова Е.А. Использование сети интернет в раскрытии и расследовании преступлений / Е.А. Гончарова // Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Юридические науки». – 2009. – Т. 22 (61). – № 1. – С. 310–315.

6. Глушко В.М. Кибернетика. Вопрос теории и практики / В.М. Глушко. – М.: Наука, 1986. – 488 с.

7. Игошин В.В. Интегральная природа науки криминалистики и ее проявление в криминалистической технике: дисс. … канд. юрид. наук. Ижевск, 2005. – 192 с.

8. Керимов Д.А. Кибернетику на службу укрепления социалистической законности / Д.А. Керимов // Кибернетика и право. – М.: Знание. – 1970. – С. 5–10

9. Рутковская М.В. Проблемы информации в поле кибернетики / М.В. Рутковская // Философские проблемы информационных технологий и киберпространства. – 2010. – № 1. – С. 193–197.

10. Самороковский В.М., Шабалин В.Е. Криминалистика и кибернетика / В.М. Самороковский, В.Е. Шабалин // Вестник Московского университета. – М.: Изд-во Моск. ун-та. – 1983. – № 5. – С. 87–88.

11. Хакин Г. Синергетика. Иерархии неустойчивостей в самоорганизующихся системах и устройствах: Монография / Г. Хакин. – М.: Изд-во Мир, 1985. – 424 с.

4. Учебная и учебно-методическая литература:

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учеб. для вузов / под ред. проф. Р.С. Белкина. – М.: НОРМА-ИНФРА, 2000. – 990 с.

2. Гончаров М.В. Введение в Интернет: в 9 частях: Учебное пособие / М.В. Гончаров, Я.Л. Шрайберг. – М.: ГПНТБ России, – 2000. – 78 с.

3. Крылова В.В. Современная криминалистика. Правовая информатика и кибернетика / В.В. Крылов. – М.: ЛексЭст, – 2007. – 288 с.

4. Мезеря Д.А., Пахомов С.В. Методика расследования мошенничеств, совершаемых посредством сотовой связи лицами, отбывающими наказание в местах лишения свободы. Учебное пособие. Краснодар: КрУ МВД России, – 2014. – 86 с.

5. Пескова С.А. Сети и телекоммуникации: Учебное пособие для вузов / С.А. Пескова, А.В. Кузин, А.Н. Волков. – М.: Академия, – 2006. – 352 с.

6. Полевой Н.С. Криминалистика и кибернетика / Н.С. Полевой. – М.: Изд-во Моск. ун-та, – 1982. – 206 с.

7. Розанова Л.В. Основы кибернетики: Конспект лекции / Л.В. Розанова. – Омск: Изд-во ОмГТУ, – 2009. – 60 с.

5. Электронные и иные справочные ресурсы:

1. Бозов А.А. Использование возможностей сотовой связи при раскрытии и расследовании преступлений: Методические рекомендации. 2013. Режим доступа: http://pravorub.ru/personal/30734.html

2. Бондаренко И. Исследование истории и темпов развития социальных сетей в мире. Режим доступа: http://www.timetoast.com/timelines/социальные-сети-история-развития

3. Википедия – свободная энциклопедия. Режим доступа: https://ru.wikipedia.org/wiki/Заглавная_страница

4. Все о социальных сетях. Влияние на человека. Режим доступа:

http://secl.com.ua/article-vse-o-socialnyh-setjah-vlijanije-na-cheloveka.html

5. Данные консалтингового агентства AC&M Consulting. Режим доступа: http://www.bit.prime-tass.ru/news/show.asp?id=62789&ct=Telecom

6. Информационно-правовая справочная система ГАРАНТ ПЛЮС. Режим доступа: http://www.garant.ru/

7. Исследования аналитической компании Royal Pingdom. Режим доступа: http://quty.ru/news/rezultati-issledovaniya

8. Криминалистическая кибернетика. Режим доступа: http://kbugaev.narod.ru/libfree/diplom/Kibernet.htm

9. Официальный сайт МВД РФ. Режим доступа: http://www.mvd.ru/mvd/structure/

10. Принцип работы электронной почты – E-Mail. Режим доступа: http://it-student.com.ua/servisy-i-slujby/main/princip-raboty-elektronnoi-pochty-e-mail.html

11. Рейтинг провайдеров (г.Краснодар). Режим доступа: http://www.2ip.ru/

12. Селиванов Н.А., Танасевич В.Г., Эйсман А.А. Советская криминалистика. Теоретические проблемы. – Москва: Юридическая литература, 1978. Режим доступа: http://зачётка.рф/book/4357/189390/%C2%A7%201.%20%D0%9F%D1%80%D0%B5%D0%B4%D0%BC%D0%B5%D1%82%20%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B8.html

13. Социальные сети. Скрытая угроза для пользователей социальной сети. Режим доступа: http://pro-spo.ru/social/3232-soczialnye-seti-skrytaya-ugroza

14. Социальные сети. Режим доступа: http://pro-spo.ru/social/3232-soczialnye-seti-skrytaya-ugroza

15. Список операторов сотовой связи. (по состоянию на 30 июня 2013 года). Режим доступа: http://ru.wikipedia.org/wiki/Вымпел-Коммуникации#.D0.A1.D0.BE.D1.82.D0.BE.D0.B2.D0.B0.D1.8F_.D1.81.D0.

B2.D1.8F.D0.B7.D1.8C

16. Статья «Что такое IP адрес». Режим доступа: http://2ip.ru/article/ip/?PHPSESSID=mv7hm87rdm8prdvr9f3mmdfr07

17. Технические средства передачи информации Режим доступа: http://ru.wikiversity.org/wiki/0:%D0%A2%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D1%81%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%B0_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8

18. Филиппов А.Г., Агафонов В.В. Криминалистика: конспект лекций. – Москва, 2009. Режим доступа: http://lib.rus.ec/b/204003

19. Электронная почта. Основные возможности. Структура почтового сообщения. Программные средства. Режим доступа: http://www.yaklass.ru/materiali?mode=cht&chtid=465

20. Электронный учебник по дисциплине: «Менеджмент» - СПбГУ ИТМО, кафедра менеджмента. Абакумов В.В., Голубев А.А., Кустарев В.П., Подлесных В.И., Прохоров Ю.К., Тюленев Л.В. Режим доступа: http://de.ifmo.ru/bk_netra/page.php?tutindex=3&index=16

21. IANA — Number Resources (количество ресурсов). Режим доступа: http://www.iana.org/numbers

Приложение 1

АНКЕТА
по изучению эффективности деятельности правоохранительных органов по раскрытию, расследованию и предупреждению преступлений при помощи внедрения современных информационных технологий

Рассматриваемое положение	% от опрошенных
Установочная часть	
1. Рассматриваемые анкеты	100%
2. Стаж работы в следствии:	
- от 1 года до 5 лет	42 %
- от 5 лет до 15 лет	52 %
- от 15 лет до 25 лет	6 %
- свыше 25 лет	-
3. Как Вы оцениваете Ваш профессиональный уровень:	
- недостаточный (не позволяет решать служебные задачи)	2 %
- ниже среднего (позволяет осуществлять служебную деятельность, но остро чувствуется нехватка профессиональных знаний)	-
- средний (позволяет решать основные служебные задачи)	22 %
- выше среднего (позволяет решать почти все служебные задачи)	60 %
- отличный (позволяет решать любые служебные задачи)	16 %
Анкетная часть:	
1. Высшее образование Вами было получено в:	
- ведомственном профильном учреждении	50 %
- образовательном учреждении с гражданско-правовым уклоном	11 %
- образовательном учреждении с уголовно-правовым уклоном	32 %
- образовательном учреждении с технико-правовым уклоном	5 %
- образовательном учреждении с финансово-экономическим уклоном	2 %
- иное	-
2. По Вашей специальности предполагалось обучение информационным технологиям (работа с компьютером и компьютеризированными системами)?	
- да	71 %
- нет	16 %
- да, но уровень полученных знаний не всегда помогает справиться с решением задач в области информационных технологий	13 %
- иное	-
3. Каков Ваш уровень владения компьютером	
- низкий	-
- средний	16 %
- уверенный пользователь	78 %
- профессионал	6 %
- иное	-

4. В своей профессиональной деятельности Вы используете следующее программное обеспечение:	
- текстовый редактор	23 %
- графический редактор	7 %
- интернет браузер	19 %
- почтовые оболочки	9 %
- планировщик деятельности (органайзеры)	6 %
- ауди-видео проигрыватели	17 %
- конверты файлов	11 %
- программы восстановления утраченных данных с электронных носителей	6 %
- иное	2 %
5. Есть ли у Вас возможность использовать в своей деятельности информационную сеть Интернет	
- есть, я активно использую интернет в своей профессиональной деятельности	78 %
- есть, однако необходимость его использования в моей деятельности отсутствует	-
- нет, так как не оснащен соответствующим необходимым оборудованием	17 %
- нет, так как не обладаю необходимыми навыками работы на компьютере	-
- Иное (используют личное оборудование)	5 %
6. Считаете ли Вы эффективным использование интернета в раскрытии, расследовании и предупреждении преступлений?	
- да, возможности интернета могут быть эффективно использованы в данных целях	68 %
- считаю, что возможности использования интернета в данных целях переоценены, однако он может оказаться неплохим подспорьем для сотрудника	19 %
- нет, использование интернета абсолютно в целях раскрытия, расследования и предупреждения преступлений абсолютно не эффективно	13 %
- иное (указать)	-
7. Использовали ли Вы информационную сеть (интернет) для розыска скрывшихся подозреваемых, выявления фигурантов или доказательств совершенных преступлений?	
- да, использовал для выявления лиц, виновных в преступном деянии	24 %
- да, использовал для получения доказательств совершенного преступления	35 %
- да, использовал для розыска скрывшихся подозреваемых (обвиняемых)	24 %
- нет, не использовал, так как не вижу в этом необходимости	15 %
- нет, не использовал, так как не обладаю соответствующими навыками его использования в целях решения служебных задач	-
- Иное (указать)	2 %
8. Используя возможности информационной сети Интернет в целях раскрытия, расследования и предупреждения преступлений вы:	

- делал(а) всю работу самостоятельно	68 %
- привлекал(а) сотрудников УСТМ	32 %
- иное	-
9. Известно ли Вам, каким образом организован доступ к информационным порталам сети Интернет, что представляет собой IP-адрес пользователя и процедура его присвоения?	
- да, известно. Имею опыт использования данных знаний в целях установления местоположения пользователя глобальной сети Интернет	21 %
- да, имею общие представления по данному вопросу	63 %
- нет, не имею соответствующих знаний в данной области	16 %
- иное (указать)	-
10. Приходилось ли Вам использовать информацию, имеющуюся в базе компаний-владельцев социальных сетей (одноклассники, вконтакте, фейсбук и т.п.) в оперативных и иных целях расследования?	
- да, использовал данные информационные базы в служебной деятельности	64 %
- нет, не использовал	31 %
- не использовал, так как не имею соответствующих навыков	5 %
- иное (указать)	-
11. Сталкивались ли Вы с необходимостью осуществления выемки информации (почтовой корреспонденции), содержащейся в базе электронных почтовых ресурсов (mail, yandex, rambler и т.п.)?	
- да, сталкивался с такой необходимостью и производил соответствующее следственное действие	60 %
- необходимость была, однако выемка не производилась в виду сложившихся затруднений	34 %
- не задумывался раньше о такой возможности	6 %
- иное (указать)	-
12. Приходилось ли Вам использовать в целях раскрытия, расследования и предотвращения преступлений возможности сотовых операторов связи?	
- да, использовал для получения информации о соединения между абонентами	40 %
- да, использовал для установления местоположения абонента в момент соединения	29 %
- да, использовал для получения информации об абоненте	29 %
- нет, не приходилось	2 %
- иное (указать)	-
13. Допустимо ли, по Вашему мнению, использовать возможности глобальной сети Интернет в целях организации официальной переписки сотрудника с процессуальными субъектами расследования?	
- да, это позволит оптимизировать деятельность следователя и расширить возможные направления обмена информацией в процессе расследования	59 %
- да, но это должно быть нормативно урегулировано	37 %
- нет, так как это снижает деловой статус сотрудника и может вызвать недоверие со стороны граждан	2 %
- нет, так как это кажется неэтичным	2 %

14. Считаете ли Вы, что владение сотрудниками ОВД информационными технологиями, знание законов кибернетики (законов информационных потоков) очень важно для реализации разного рода служебных задач?	
- да, я согласен(а) с этим	74 %
- нет, я так не считаю	2 %
- иное (указать)	24 %
15. С каким из нижеперечисленных высказываний Вы согласны?	
- знания работы на компьютере – это важные и обязательные знания, без которых затрудняется современная профессиональная деятельность	54 %
- знания работы на компьютер – это второстепенные знания, без которых возможно построение своей современной профессиональной деятельности	12 %
- Интернет – это мощный ресурс получения оперативной и достоверной информации	20 %
- Интернет – это мощный ресурс, объединивший огромное количество людей	14 %

Приложение 2

МВД РФ
ГЛАВНОЕ УПРАВЛЕНИЕ
ВНУТРЕННИХ ДЕЛ
по Энской области
ГЛАВНОЕ СЛЕДСТВЕННОЕ
УПРАВЛЕНИЕ
000000, г. Энск, ул.
Коммунистическая, 17
тел. 000-00-00 факс 000-00-00
от 01.01.2014*г.* **№ *8/04 –_____СЧ***
на №_____

Генеральному директору
ООО «Одноклассники»
Киселеву М.Е.

115114 г. Москва, Дербеневская набережная,
д. 7 стр. 17, этаж 3, помещение 1
(вход через 10 строение)

В СЧ ГСУ при ГУВД по Энской области расследуется уголовное дело №0000001 по подозрению Вихшенберга Р.И. в совершении преступления, предусмотренного ч.4 ст.159 и п. «б» ч.2 ст.199 УК РФ.

В ходе предварительного расследования подозреваемый Вихшенберг Р.И. нарушил избранную в отношении него меру пресечения в виде подписки о невыезде и надлежащем поведении и скрылся от органов предварительного следствия.

21.12.2013 года объявлен розыск подозреваемого Вихшенберга Р.И., который поручен сотрудникам УВД по г.Энску, заведено розыскное дело №000086 от 22.12.2013 года.

В ходе предварительного расследования уголовного дела получена информация о том, что Вихтенберг Рафаэль Илларионович 25.07.1973 года рождения, является активным пользователем социальной сети «Одноклассники».

На основании вышеизложенного, с целью установления местонахождения Вихшенберга Р.И., прошу Вас предоставить следующую информацию о пользователе, зарегистрированном в социальной сети «Одноклассники» как Рафаэль Вихтенберг, 40 лет, Энск, Россия (до 18.12.2013г.), а с 18.12.2013г. переименованного как Рафик Потапов, 40 лет, Энск, Россия: **используемый IP-адрес и время выхода в сеть в период с 18.12.2013 года по настоящее время**; указанные анкетные данные (ФИО, адрес местожительства, место работы, e-mail, номер телефона, круг общения (друзья) и другую имеющуюся информацию).

Заранее благодарю за содействие.

Приложение: - распечатка страницы социальной сети «Одноклассники», используемой Вихтенбергом Р.И. по состоянию на 17.12.2013г. на 1 листе; - распечатка страницы социальной сети «Одноклассники», используемой Вихтенбергом Р.И. по состоянию на 25.12.2013г. на 1 листе.

Следователь следственной части ГСУ
при ГУВД по Энской области
капитан юстиции О.Н. Жарков

Приложение 3

МВД РФ
ГЛАВНОЕ УПРАВЛЕНИЕ
ВНУТРЕННИХ ДЕЛ
по Энской области
ГЛАВНОЕ СЛЕДСТВЕННОЕ
УПРАВЛЕНИЕ
000000, г. Энск, ул.
Коммунистическая, 17
тел. 000-00-00 факс 000-00-00
от 15.01.2014*г.* **№ *8/04 –_____СЧ***
на №_____

Руководителю
ОАО «ИнфоТеКС Таганрог Телеком»

Ростовская область, г. Таганрог,
ул. Октябрьская, д. 19

В СЧ ГСУ при ГУВД по Энской области расследуется уголовное дело №0000001 по подозрению Вихшенберга Р.И. в совершении преступления, предусмотренного ч.4 ст.159 и п. «б» ч.2 ст.199 УК РФ.

В ходе предварительного расследования подозреваемый Вихшенберг Р.И. нарушил избранную в отношении него меру пресечения в виде подписки о невыезде и надлежащем поведении и скрылся от органов предварительного следствия.

21.12.2013 года объявлен розыск подозреваемого Вихшенберга Р.И., который поручен сотрудникам УВД по г.Энску, заведено розыскное дело №000086 от 22.12.2013 года.

В ходе предварительного расследования уголовного дела получена информация о том, что Вихтенберг Рафаэль Илларионович 25.07.1973 года рождения, является активным пользователем социальной сети «Одноклассники».

На основании вышеизложенного, с целью установления местонахождения Вихшенберга Р.И., прошу Вас предоставить сведения о пользователе (адрес местонахождения, анкетные данные), выходившем в сеть Интернет через Ваш Интернет-провайдер под следующими IP-адресами в указанное время:

Дата, время	IP-адрес
18.12.2013г. 22:46:08	84.51.220.84
19.12.2013г. 00:49:02	84.51.208.124
19.12.2013г. 10:24:28	84.51.210.127
25.12.2013г. 14:41:00	84.51.220.157
28.12.2013г. 01:00:59	84.51.221.8
28.12.2013г. 16:12:16	84.51.219.72
30.12.2013г. 09:52:12	84.51.222.209
31.12.2013г. 15:02:26	84.51.216.8
02.12.2013г. 00:42:00	84.51.219.4
08.12.2013г. 14:45:25	84.51.215.142
10.12.2013г. 19:04:56	84.51.220.282

Заранее благодарю за содействие.

Следователь следственной части ГСУ
при ГУВД по Энской области
капитан юстиции О.Н. Жарков

Приложение 4

МВД РФ
ГЛАВНОЕ УПРАВЛЕНИЕ
ВНУТРЕННИХ ДЕЛ
по Энской области
ГЛАВНОЕ СЛЕДСТВЕННОЕ
УПРАВЛЕНИЕ
000000, г. Энск, ул.
Коммунистическая, 17
тел. 000-00-00 факс 000-00-00
от 15.01.2014*г.* **№ *8/04 –_____СЧ***
на №_____

Генеральному директору
филиала ОАО «ВымпелКом»
в Краснодарском крае

г. Краснодар,
ул. Калинина, д.341, офис 404

Следственной частью ГСУ при ГУВД по Энской области расследуется уголовное дело №0000001 по подозрению Вихшенберга Р.И. в совершении преступления, предусмотренного ч.4 ст.159 и п. «б» ч.2 ст.199 УК РФ.

В связи с расследованием данного уголовного дела прошу предоставить:

1) сведения о полных анкетных данных лица и используемый(ые) им абонентский(ие) номер(а), использовавшего сотовый телефон с IMEI: 351290007972020, в период с 01 июля 2013 года по настоящее время;

2) сведения о том, зарегистрирован или нет в обслуживаемой Вами сотовой сети абонентский номер 8-958-678-89-12 (если был зарегистрирован ранее и передался в иную сеть, то когда и в какую сеть был передан). Если зарегистрирован (был зарегистрирован), также предоставить сведения о полных анкетных данных лица, на которое зарегистрирован данный абонентский номер (в случае изменения владельца данного абонентского номера также прошу указать какие изменения вносились, в какой период);

3) сведения о том, зарегистрирована или нет в обслуживаемой Вами сотовой сети SIM-карта номер 897857-925854-621453e+. Если зарегистрирована, прошу предоставить сведения о полных анкетных данных лица, на которое зарегистрирована данная SIM-карта и присвоенный ей абонентский номер (в случае изменения владельца данного абонентского номера также прошу указать какие изменения вносились, в какой период);

4) сведения о зарегистрированных в вашей сотовой сети абонентских номерах на имя гражданина Вихтенберга Рафаэля Илларионовича 25.07.1973 года рождения.

Следователь следственной части ГСУ
при ГУВД по Энской области
капитан юстиции О.Н. Жарков

Приложение 5

"_____"
(согласен, не согласен)
Заместитель начальника Следственной части
Главного следственного управления
при ГУВД по Энской области
полковник юстиции
_____А.Ф. Миронов
"_____" _____2014 года

ПОСТАНОВЛЕНИЕ
о возбуждении перед судом ходатайства о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами

г. Энск 9 января 2014 года

Следователь следственной части ГСУ при ГУВД Энской области капитан юстиции Жарков О.Н., рассмотрев материалы уголовного дела №0000001,

У С Т А Н О В И Л:

Настоящее уголовное дело возбуждено по подозрению Вихшенберга Р.И. в совершении преступления, предусмотренного ч.4 ст.159 и п. «б» ч.2 ст.199 УК РФ.

В ходе расследования уголовного дела установлено, что в июле 2013 года Вихштенберг Р.И. и Старин А.Т. достигли договоренности, согласно которой Старин А.Т. обязался передать Вихштенбергу Р.И. денежные средства, а Вихштенберг Р.И. приобрести на них контрольный пакет акций ЗАО «Николаевское». В связи с указанной договоренностью в августе 2013 года в г.Энске Вихштенберг Р.И. получил от Старина А.Т. 25 векселей Сбербанка РФ номиналом 1000000 рублей и 29000000 рублей наличными. Однако на полученные денежные средства Вихштенберг Р.И. акции Старину А.Т. не приобрел, а распорядился ими по собственному усмотрению, а именно приобрел на свое имя акции ЗАО «Неберджай». Завладев денежными средствами, Вихштенберг Р.И. от Старина А.Т. скрылся, денежные средства не возвратил.

21.12.2013 года объявлен розыск подозреваемого Вихшенберга Р.И., который поручен сотрудникам УВД по г.Энску, заведено розыскное дело №000086 от 22.12.2013 года.

В ходе предварительного следствия установлено, что подозреваемый Вихтенберг Рафаэль Илларионович 25.07.1973 года рождения, зарегистрированный по адресу: г.Энск, ул.Бегемотова, д.21, кв.5 пользовался сотовым телефоном с абонентским номеров 89025411412 сотовой связи сети «БИЛАЙН». Кроме того, из ОРЧ (по линии БЭП) получена информация о том, что Вихштенберг Р.И. также пользовался телефоном с абонентским номером 89096458713 сотовой связи сети «БИЛАЙН».

Кроме того, в ходе расследования уголовного дела получены данные о том, что Вихштенберг Р.И. поддерживает связь со своей женой Кириковой

Элеонорой Поликарповой, 12.04.1978 года рождения, пользующейся сотовым телефоном с абонентским номером 89097548596 сотовой связи сети «БИЛАЙН».

С целью установления возможных контактов подозреваемого Вихштенберга Р.И., обстоятельств совершения преступления, а также установления его местонахождения, необходимо получить сведения о владельцах указанных абонентов оператора сотовой связи «БИЛАЙН» ОАО «ВымпелКом» и детализацию телефонных переговоров данных абонентов, с указанием местонахождения абонента в момент звонков (номер соты, район ее расположения).

На основании изложенного и руководствуясь ст.165, 186^{1} УПК РФ,

П О С Т А Н О В И Л:

Ходатайствовать перед районным судом г.Энска о разрешении выдачи информации оператором сети «БИЛАЙН» ОАО «ВымпелКом»:

- о том, в каких мобильных телефонах (номер IMEI) использовались сим-карты с абонентскими номерами 89025411412 и 89096458713;

- предоставить протоколы детализации телефонных соединений абонентов, сим-карты которых помещались в телефоны, в которых использовались сим-карты с абонентскими номерами 89025411412 и 89096458713 за период с 18.12.2013 года по настоящее время.

- предоставить протоколы детализации телефонных соединений абонентов 89025411412, 89096458713 и 89097548596 в период с 18.12.2013 года по настоящее время с указанием местонахождения абонента в момент звонков (номер соты, район ее расположения).

Следователь следственной части ГСУ
при ГУВД по Энской области
капитан юстиции О.Н. Жарков

Приложение 6

"_____"
(согласен, не согласен)
Заместитель начальника Следственной части
Главного следственного управления
при ГУВД по Энской области
полковник юстиции
_____А.Ф. Миронов
"_____" _____2014 года

ПОСТАНОВЛЕНИЕ
о возбуждении перед судом ходатайства
о производстве выемки предметов и документов, содержащих государственную или иную охраняемую законом тайну

г. Энск 9 января 2014 года

Следователь следственной части ГСУ при ГУВД Энской области капитан юстиции Жарков О.Н., рассмотрев материалы уголовного дела №0000001,

У С Т А Н О В И Л:

Настоящее уголовное дело возбуждено по подозрению Вихшенберга Р.И. в совершении преступления, предусмотренного ч.4 ст.159 и п. «б» ч.2 ст.199 УК РФ.

В ходе расследования уголовного дела установлено, что в июле 2013 года Вихштенберг Р.И. и Старин А.Т. достигли договоренности, согласно которой Старин А.Т. обязался передать Вихштенбергу Р.И. денежные средства, а Вихштенберг Р.И. приобрести на них контрольный пакет акций ЗАО «Николаевское». В связи с указанной договоренностью в августе 2013 года в г.Энске Вихштенберг Р.И. получил от Старина А.Т. 25 векселей Сбербанка РФ номиналом 1000000 рублей и 29000000 рублей наличными. Однако на полученные денежные средства Вихштенберг Р.И. акции Старину А.Т. не приобрел, а распорядился ими по собственному усмотрению, а именно приобрел на свое имя акции ЗАО «Неберджай». Завладев денежными средствами, Вихштенберг Р.И. от Старина А.Т. скрылся, денежные средства не возвратил.

21.12.2013 года объявлен розыск подозреваемого Вихшенберга Р.И., который поручен сотрудникам УВД по г.Энску, заведено розыскное дело №000086 от 22.12.2013 года.

В ходе проведенных оперативно-розыскных мероприятий установлено, что подозреваемый Вихтенберг Рафаэль Илларионович 25.07.1973 года рождения, зарегистрированный по адресу: г.Энск, ул.Бегемотова, д.21, кв.5 для связи с привычным кругом общения использует электронный почтовый ящик illarion-rafik@mail.ru, зарегистрированный на сервере ООО «МЕЙЛ.РУ». Кроме того, есть основания полагать, что данный почтовый ящик также использовался для обмена электронными почтовыми письмами при совершении сделки, направленной на приобретение акций ЗАО «Неберджай».

С целью установления возможных контактов подозреваемого Вихштенберга Р.И., обстоятельств совершения преступления, а также установления его местонахождения, необходимо получить сведения о владельце

указанного почтового аккаунта (illarion-rafik@mail.ru), а также изъять электронные почтовые письма, отправленные с данного почтового ящика и полученные на него за период с 01.07.2013 года по настоящее время, хранящиеся на серверах ООО «МЕЙЛ.РУ», расположенного по адресу: г. Москва, Ленинградский проспект, д. 47, стр. 2.

На основании изложенного и руководствуясь ст. 38, частью первой ст. 165, частями первой, второй и четвёртой ст. 182 и ст. 183 УПК РФ,

ПОСТАНОВИЛ:

Ходатайствовать перед районным судом г. Энска о производстве выемки сведений о владельце почтового аккаунта illarion-rafik@mail.ru, электронных почтовых писем, отправленных с данного почтового ящика и полученные на него за период с 01.07.2013 года по настоящее время, хранящиеся на серверах ООО «МЕЙЛ.РУ», расположенного по адресу: г. Москва, Ленинградский проспект, д. 47, стр. 2.

Следователь следственной части ГСУ
при ГУВД по Энской области
капитан юстиции О.Н. Жарков