**УДК 34** **Юридические науки**

***Малышев Константин Сергеевич,*** *преподаватель кафедр оперативно-разыскной деятельности ОВД, Уральский юридический институт МВД России, Россия, г. Екатеринбург*

# ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**Аннотация:** В данной статье рассматриваются актуальные проблемы оперативных подразделений по борьбе с преступностью в сфере информационных технологий. Анализируются статистические данные, опубликованные прокуратурой РФ, о количестве преступлений в сфере ИКТ. А также рассматриваются правовые особенности, которые необходимо знать сотрудникам оперативных подразделений для проведения оперативных комбинаций, заведения дел оперативного учета и документирования проводимых мероприятий.

**Ключевые слова:** информационные технологии, оперативные подразделения, учреждения связи, интернет-провайдер, оперативно-розыскные мероприятия, снятие информации с технических каналов связи, получение компьютерной информации.

**Annotation:** This article discusses the actual problems of operational units to combat crime in the field of information technology. Statistical data published by the Prosecutor's office of the Russian Federation on the number of crimes in the field of ICT are analyzed. And also examines the legal aspects that you need to know to employees of operational units for operational combinations, the institution of operational records and documentation of activities.

**Keywords:** information technology, operational units, communication institutions, Internet service provider, operational search activities, removal of information from technical communication channels, obtaining computer information.

Развитие информационно-вычислительной техники позволяет современному обществу работать со значительным массивом данных, упростить многие процессы, одним словом, повышает работоспособность общества. Но стоит отметить и ряд негативных факторов, которые обусловлены значительной степенью цифровизации и интернетизации современного общества. К данным фактором целесообразно отнести, такие явления как:

1. рост угрозы утечки персональных данных;
2. развитие отдельного криминального сегмента, специализирующегося на преступлениях в сфере информационных технологий;
3. формирование условий для развития наркорынка, рынка поддержки и финансирования терроризма, а также иных рынков для оборота объектов, изъятых из гражданского оборота или оборот которых ограничен;
4. развитие условий для совершения мошенничеств с использованием электронных средств платежа;
5. развитие рынков отмывания и легализации денежных средств или иного имущества, добытых преступным путем;
6. формирование условий для образования финансовых пирамид и др. [1].

Совокупность данных факторов оказывает сильное воздействие на общество, а также создает угрозу экономической безопасности страны и её национальным интересам. С течением времени криминальный контингент в данной отрасли только развивается и учится совершать новые преступления с различными способами маскировки своих преступных посягательств. О развитии преступности в сфере информационно-коммуникационных технологий свидетельствуют данные с 3 встречи прокурорских служб БРИКС, которая состоялась 24 августа 2017 года [2]. На данной встрече Юрий Чайка

Генеральный прокурор РФ отметил, что в Российской Федерации число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 по 2016 год увеличилось в 6 раз (с 11 тыс. до 66 тыс.) [3].

За 2017 год число преступлений в данной сфере увеличилось с 65 949 до 90 587. А за январь-сентябрь 2018 года было зарегистрировано 121 247 преступлений в сфере информационно-коммуникационных технологий, но это далеко не предел, в 2019 году только за первые восемь месяцев было зарегистрировано 180 153 преступления в данной сфере, что на 66,8% выше показателя за аналогичный период в 2018 году [4].

Из представленного массива данных видно, что эта сфера создает действительно серьёзную угрозу для всего общества. Такая тенденция к росту количества преступлений в сфере информационных технологий коррелирует с рядом объективных и субъективных факторов. К данным фактором можно отнести:

1. отсутствие превентивных мер в отношении населения (своевременное информирование, проведение профилактических мероприятий по формированию знаний в данной сфере у населения);

2. отсутствие своевременных апгрейдов систем защиты информации от несанкционированного доступа или иного аппаратно-программного комплекса защиты информации;

3. законодательные пробелы, которые позволяют избегать ответственности за совершенные посягательства;

4. недостаточность знаний и технической оснащенности сотрудников правоохранительных органов;

5. разработка различных средств маскировки преступлений (VPN, криптовалюта, публичный wi-fi и др.)

6. недостаточность знаний сотрудников правоохранительных органов нормативной и технической документации в данной сфере.

Стоит отметить, что данная категория преступлений отличается особой сложностью, которая обусловлена рядом факторов, например:

1. отсутствие конкретного лица, в отношении которого ведется первичная проверка в рамках дел оперативного учета;

2. наличие хороших средств маскировки своей деятельности (VPN, криптовалюта, публичный wi-fiи др);

3. возможность действий злоумышленника на значительных расстояниях;

4. хорошая техническая оснащенность;

5. анонимное содействие должностных лиц (например, сотрудник банка осуществляет передачу баз данных злоумышленнику);

6. техническое обеспечение оперативных подразделений;

7. сложность предварительного планирования оперативных комбинаций в данной отрасли и др.

Таким образом, сотрудникам оперативных подразделений следует хорошо разбираться в данной сфере для благоприятного разрешения данной категории дел. Стоит отметить, что в ст. 10.1 ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ закреплены обязанности организатора распространения информации в сети «Интернет», данная норма закрепляет случаи предоставления различной информации органам исполнительной власти РФ уполномоченным осуществлять оперативно-розыскную деятельность, а также обязанности по хранению и декодированию соответствующей информации [5].

Вопрос документирования и принятия качественного оперативного решения по поступившей первичной информации, которая подлежит проверке, сотрудникам оперативных подразделений необходимо владеть соответствующей терминологией и положениями закона, которые закреплены в ФЗ «О связи» от 07.07.2003 №126-ФЗ. Данные положения и терминология помогут дать правильную юридическую оценку тем или иным явлениям, а также сформировать корректный запрос администрации организаций связи и интернет-провайдеру.

Кроме всего, необходимо ознакомиться с положениями ФЗ «О персональных данных» от 27.07.2006 №152-ФЗ, которые позволят сформировать соответствующие знания об использовании персональных данных в оперативно-розыскной деятельности при раскрытии и изобличении преступлений данной категории.

Также сотрудникам оперативных подразделений необходимо понимать отличие таких ОРМ как получение компьютерной информации (ПКИ) и снятие информации с технических каналов связи (СИТКС) друг от друга, от понимания различия данных оперативно-розыскных мероприятий и их назначения будет зависеть целесообразность применения сотрудником того или иного мероприятия.

Снятие информации с технических каналов связи — это оперативно-розыскное мероприятие, которое направлено на изъятие информации с электронных носителей информации различных видов, с помощью соответствующих технических средств и специалиста, который обладает достаточным уровнем квалификации для осуществления данных мероприятий.

Зачастую многие сотрудники не понимают в чем отличие между ПКИ и СИТКС, а также оспаривают целесообразность включения оперативно-розыскного мероприятия получение компьютерной информации в перечень оперативно-розыскных мероприятий, закрепленных в ст. 6 ФЗ «Об оперативно-розыскной деятельности» от 12 августа 1995 №144-ФЗ [6].

Однако, данное ОРМ необходимо для формализации мероприятий по получению информации от учреждений связи, Интернет-провайдера и других организаций, которая составляет охраняемую законом тайну или получение которой нарушает конституционные права человека и гражданина, предусмотренные ст. 23, 24 Конституцией РФ, а также для получения которой не требуется участие специалиста и применение специальных технических средств. Например, получение информации от интернет-провайдера о движении интернет-трафика.

Для организации эффективного оперативного обслуживания данной линии работы сотрудникам оперативных подразделений следует выполнить следующие мероприятия:

1. изучить нормативную и техническую документацию регламентирующую данную отрасль;

2. составить перечень лиц на территории обслуживания, чьи способности могут потенциально быть применены для совершения преступных посягательств в сфере информационно-коммуникационных технологий;

3. завести накопительное дело на сферу оперативного обслуживания в целом;

4. определить принципы и режим оперативного обслуживания закрепленных объектов;

5. ознакомиться с основными способами совершения преступлений в данной отрасли, понять механику и алгоритм действий злоумышленника;

6. сформировать гласные и негласные источники получения информации;

7. сформировать базу специалистов по данной линии оперативной работы, приоритет к лицам, которые располагают базами данных возможных объектов оперативного обслуживания, а также лица с большими техническими возможностями;

8. провести консалтинговые мероприятия с лицами сведущими в данной области, например, сотрудники отдела безопасности учреждений связи и иных организациях специализирующихся на оказании услуг в сфере информационно-коммуникационных технологий.

Источники оперативной информации следует формировать среди лиц, которые могут располагать достоверной информацией, которые имеют широкий спектр связей в данной отрасли, которые имеют доступ к различным серверам и т. д.

Для максимизации эффективности работы по данной линии требуется слаженная работа различных оперативных подразделений, а также социально ответственная позиция со стороны организаций, предоставляющих услуги в

данной сфере и лиц, организующих работу различных систем, приложений, сервисов, серверов и т. д. Не стоит забывать об осуществлении превентивных мер в отношении населения, а именно различные профилактические беседы, своевременные смс рассылки со значимой информацией и др.

**Библиографический список:**

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ// www.consultant.ru.

2. Конституция Российской Федерации от 12.12.1993// www.consultant.ru.

3. Федеральный закон "О связи" от 07.07.2003 N 126-ФЗ// www.consultant.ru.

4. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ// www.consultant.ru.

5. Новостной портал «ПРАВО.RU» // pravo.ru.

6. Федеральный закон "Об оперативно-розыскной деятельности" от 12.08.1995 N 144-ФЗ// www.consultant.ru.