МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Казанский юридический институт

ВЫЯВЛЕНИЕ, ПРЕСЕЧЕНИЕ И ДОКУМЕНТИРОВАНИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 159.6 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Методические рекомендации

Казань • 2017

Рецензенты:

- ;
- .

В96 Выявление, пресечение и документирование преступлений, связанных с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации: методические рекомендации / С.Н. Миронов [и др.] – Казань: КЮИ МВД России, 2017. – 65 с.

Методические рекомендации подготовлены :
- к.и.н., доцентом С. Н. Мироновым (общая редакция);
- д.э.н., доцентом И. В. Жуковской (§1 главы 1);
- к.ю.н. А. И. Музеевым (введение, глава 2, заключение);
- Н. М. Сафиным (§2 главы 1);
- М.И. Гараевым, (§2 главы 2);
- к.э.н., М.Н. Сафиуллиным (§2 главы 2).

В методических рекомендациях рассматриваются вопросы выявления, пресечения и раскрытия преступлений, предусмотренных ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». Исследованы проблемы уголовно-правовой квалификации данных преступлений, дана их криминологическая характеристика,

Предназначено для сотрудников оперативных подразделений органов внутренних дел, а также курсантов и слушателей образовательных организаций системы МВД России при изучении дисциплин «Оперативно-розыскная деятельность органов внутренних дел», «Криминология», «Практикум по особенностям квалификации отдельных видов преступлений».

© Казанский юридический институт МВД России, 2017

Оглавление

Использованные обозначения и сокращения:

МВД – министерство внутренних дел
ОВД – орган(ы) внутренних дел
ОРД – оперативно-розыскная деятельность
ОРМ – оперативно-розыскные мероприятия
ПСТМ – подразделения специальных технических мероприятий;
УК – Уголовный кодекс Российской Федерации
УПК – Уголовно-процессуальный кодекс Российской Федерации
(У)ЭБиПК – (управление) экономической безопасности и противодействия коррупции

ВВЕДЕНИЕ

В современных условиях технического развития общества, ускорения информационных процессов и расширения информационного пространства компьютерные системы играют весьма значимую социальную роль. Однако наряду с положительным коммуникативным эффектом в жизни общества развитие компьютерных технологий повлекло за собой их использование в противоправной деятельности. Анализ складывающейся ситуации позволяет утверждать, что совершенствование компьютерных технологий приводит не только к ускорению развития общества, но и к расширению источников опасности для него, в том числе связанных с явлениями криминального плана.

Для киберпреступников один из самых коротких путей к деньгам – это атака на клиентов банков. Как правило, злоумышленники с помощью социальной инженерии обманным путем добиваются, чтобы жертвы сообщали свои личные данные или устанавливали вредоносное программное обеспечение (далее ПО), собирающее персональную информацию (пароли), которую они используют для доступа к своему банковскому счету. По данным «Лаборатории Касперского», в 2016 году ее антивирусы заблокировали попытки запустить вредоносное ПО, предназначенное для кражи денег через системы онлайн-банкинга, на 2 871 965 устройствах. Киберпреступники охотятся не только на клиентов банков – в последние годы наблюдается рост числа атак непосредственно на банки и другие финансовые организации.[1]

Европейское агентство по вопросам сетевой и информационной безопасности (European Union Agency for Network and Information Security, ENISA) отмечает, что в 2016 году количество мобильных угроз возросло на 150 %; в списке основных киберугроз лидируют атаки с применением вредоносного

[1] Kaspersky security bulletin 2016: развитие угроз. URL: https://press.kaspersky.com/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016_итоги.pdf (дата обращения 12.04.2017).

программного обеспечения, а среди источников таких атак называется и Россия.[1]

Сложившаяся ситуация оказала влияние и на определение приоритетов внутренней политики страны. В Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы среди прочих направлений называются и обеспечение создания и развития систем нормативно-правовой, информационно-консультативной, технологической и технической помощи в обнаружении, предупреждении, предотвращении и отражении угроз информационной безопасности граждан и ликвидации последствий их проявления.[2]

Анализ уголовной статистики свидетельствует о значительной доле зарегистрированных преступлений по ст. 159.6 УК РФ в общей массе преступлений, совершаемых с использованием компьютерной информации. Вместе с тем сотрудники органов внутренних дел осуществляют свою деятельность в текущих условиях несогласованного банковского, корпоративного и иного законодательства, отсутствия механизмов взаимодействия с коммерческими структурами и, прежде всего, банками, провайдерами, операторами сотовой связи, отвечающих современным требованиям, нехватки специалистов в сфере компьютерных технологий, способных оказать помощь в расследовании хищений, отсутствия необходимой в достаточном количестве и качестве специальной криминалистической техники (напр., аппаратно-программных комплексов) и т.п.[3]

Перечисленные и иные объективные обстоятельства затрудняют деятельность сотрудников органов внутренних дел, осуществляющих раскрытие преступлений, связанных с хищениях денежных средств, совершаемых с использованием компьютерных технологий. В то же время, как показывает практика, сотрудники, специализирующиеся на раскрытии обозначенных преступлений,

---

[1] В 2016 году число мобильных угроз возросло на 150%. URL: http://www.itsec.ru/newstext.php? news_id=114914 (дата обращения 12.04.2017).

[2] О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента РФ от 9 мая 2017 г. № 203.

[3] Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий: учебно-практическое пособие. М.: Академия управления МВД

не обладают достаточными профессиональными и специальными знаниями, умениями и навыками в выявлении хищения чужого имущества или приобретения права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации, оперативно-розыскного обеспечения предварительного расследования по уголовным делам, возбужденным по ст.159.6 УК РФ.

В связи с этим руководством ряда территориальных подразделений МВД России уделяется пристальное внимание совершенствованию профессиональной подготовки сотрудников оперативных подразделений органов внутренних дел, приобретению и закреплению ими навыков расследования хищений денежных средств с использованием компьютерных технологий, с учетом обозначенных условий. Так, УЭБиПК МВД по Республике Татарстан было инициировано исследование проблем борьбы с преступлениями, связанными с мошенничеством в сфере компьютерной информации, предусмотренных статьей 159.6 Уголовного кодекса Российской Федерации, и подготовка на этой основе методических рекомендаций.

Сформулированные авторами рекомендации по преодолению проблем, выявленных в ходе проведенного исследования, приведены с учетом современной ситуации, связанной с мошенничеством в сфере компьютерной информации, изучения ведомственной статистики, материалов исследований в области борьбы с преступлениями в сфере высоких технологий. Предложения основаны также на материалах, предоставленных отделом «К» ПБСТМ, УЭБ и ПК МВД по Республике Татарстан по преступлениям в сфере хищения денежных средств с использованием компьютерной информации. Основные выводы проведенного исследования сделаны на основании анализа действующих правовых норм отечественного уголовного, уголовно-процессуального и оперативно-розыскного законодательства, теоретических положений, материа-

---

России, Следственный департамент МВД России, 2016. С.6.

лов оперативно-розыскной практики, а также мнения практических сотрудников.

ГЛАВА 1. КРИМИНОЛОГИЧЕСКИЕ И УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ БОРЬБЫ С МОШЕННИЧЕСТВОМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Современное состояние преступности, связанной с мошенничеством в сфере компьютерной информации

Очень часто термин «киберпреступность» употребляется в качестве синонима понятия «компьютерная преступность». Несмотря на то, что эти термины очень близки, понятие «киберпреступность» (в англоязычном варианте – cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве. В работах зарубежных ученых и документах международных организаций также отдается предпочтение термину «киберпреступность».

С учетом рекомендаций экспертов ООН, а также документов иных международных организаций, сформулировано следующее определение киберпреступности и киберпреступления: Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

Киберпреступление – это виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству.

Термин «киберпреступление» охватывает весь спектр преступлений в сфере информационных технологий, будь это преступления, совершенные с помощью компьютеров, или преступления, предметом которых являются компьютеры, компьютерные сети и хранящаяся на этих носителях информация.

Компьютерное преступление – это только то преступление, которое посягает на безопасное функционирование компьютеров и компьютерных сетей, а также на обрабатываемые ими данные. Таким образом, если рассматривать соотношение этих двух понятий, то компьютерное преступление является разновидностью киберпреступления.

Основными преступными деяниями, образующими рынок киберпреступности на сегодняшний день, являются:

1) мошенничество в системах интернет-банкинга;

2) фишинг;

3) хищение электронных денег;

4) услуги обналичивания иных нелегальных доходов;

5) спам (информация о медикаментах и различной контрафактной продукции, поддельном программном обеспечении, сфере услуг, образования, туризма);

6) продажа трафика;

7) продажа эксплойтов;

8) продажа загрузок;

9) анонимизация;

10) DDoS-атаки.

Анализ статистических данных о преступности в сфере компьютерной информации показывает, что с 2006 по 2016 гг. в России количество зарегистрированных преступлений в сфере компьютерной информации (глава 28 УК РФ) выросло более чем в 300 раз.

В 2016 г. число зарегистрированных преступлений *в сфере телекоммуникаций и компьютерной информации* составило 10 227, что на 28,3 % выше показателя 2011 г. (7 974). В 2015 г. число аналогичных посягательств составило – 7 142 преступления, что на 37,2 % меньше, чем в 2010 г. (12 698). Приведенный анализ динамики числа зарегистрированных преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, свидетельствует о

том, что максимальное количество преступлений было совершено в 2013 г. (17 535 преступлений) (табл. 1).

Таблица 1

Динамика преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, зарегистрированных в Российской Федерации, и число пользователей Интернета в 2013 – 2016 гг.

	2013	2014	2015	2016
Абсолютный показатель	17 535	12 698	7 974	10 227
Темп прироста, к АППГ (%)	-	- 27,6	-37,2	28,3
Число Интернет пользователей, (млн чел.)	53,5	59,7	60,4	68,0

Прослеживаемая из представленных данных тенденция к снижению количества зарегистрированных преступлений, зафиксированная в 2013-2016 гг., вряд ли адекватно отражает реальную динамику фактической преступности. На наш взгляд, подобные процессы могут быть объяснены, с одной стороны, ослаблением контроля учетно-регистрационной дисциплины, с другой стороны – снижением активности правоохранительных органов по выявлению такого вида преступлений, поскольку действие основных факторов, обусловливающих их совершение, не уменьшилось, а, напротив, увеличилось. Вместе с тем необходимо отметить, что рост вышеуказанных преступлений в 2013 г. связан с увеличением числа Интернет-пользователей – (68,0) на 7,6 млн. Это обстоятельство дает основание полагать, что отмечаемое сокращение количества зарегистрированных преступлений носит искусственный характер.

Так, исходя из статистических данных ГИАЦ МВД России за 2016 год, структура российской компьютерной преступности выглядит следующим образом:

1. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ), -30,2 %.

2. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 21,2 %.

3. Нарушение авторских и смежных прав, совершенное с использованием компьютерных и телекоммуникационных технологий (ст.146 УК РФ), – 11,1 %.

4. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) – 9,8 %.

5. Кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ), -9,78 %.

6. Незаконные изготовление и оборот порнографических материалов или предметов, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242 УК РФ), – 6,1 %.

7. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242.1 УК РФ), – 5,3 %.

8. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 183 УК РФ), – 2,8 %.

9. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ), – 2,4 %.

10. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов, совершенное посредством компьютерных и телекоммуникационных технологии (ст. 242.2 УК РФ), – 0,5 %.

11. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 138 УК РФ) – 0,4 %.

12. Причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 165 УК РФ), – 0,2 %.

13. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) – 0,02 %.

14. Незаконные организация и проведение азартных игр, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 171.2 УК РФ), – 0,2 %.

Как следует из приведенных данных, наибольший удельный вес среди совершенных компьютерных преступлений приходится на преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), которые в данное время и составляют основу компьютерной преступности в России. Исследуя официальную статистику, можно увидеть следующую картину российской компьютерной преступности, характеризующую ее состояние.

В 2016 году в Российской Федерации по фактам совершения компьютерных преступлений были возбуждены уголовные дела: за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 1 396; создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) – 974; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) – 12; мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) – 1 352. При этом, согласно официальной статистике, динамика совершения преступлений в сфере компьютерной информации носит регрессивный характер, т.е. количество зарегистрированных, а следовательно, расследованных и направленных в суд уголовных дел из года в год неуклонно снижается. По данным ГИАЦ МВД России, общее количество преступлений в сфере компьютерной информации (зарегистрирован-

ных в текущем периоде календарного года), предусмотренных ст. 272 и ст. 273, 274 УК РФ, составило: в 2010 г. соответственно 9 489 и 2097, 4; в 2011 г. – 6 132 и 1 010, 0; в 2012 г. – 2 005 и 693, 0; в 2013 г. – 1 930 и 889, 1; в 2014 г. – 1 799 и 764, 0; в 2015 г. – 1 151 и 585, 3; в 2016 г. – 1396 и 974, 12.

Таким образом, за последние годы количество выявленных преступлений в сфере компьютерной информации сократилось почти в 5 раз (количество уголовных дел уменьшилось с 11 590 до 2 382). При этом необходимо отметить серьезные проблемы не только в выявлении преступлений в сфере компьютерной информации, но и в деятельности органов дознания и предварительного следствия при расследовании данной категории преступлений.

Например, статистика расследованных уголовных дел, возбужденных по признакам преступлений, предусмотренных ст. 273 УК РФ, показывает, что по реабилитирующим основаниям прекращены: в 2010 г. – 50, в 2011 г. – 35, в 2012 г. – 78, в 2013 г. – 163 уголовных дела; «приостановлены за нерозыском лица либо в случае неустановления лица, совершившего преступление»: в 2011 г. – 58, в 2012 г. -75, в 2013 г. – 108, в 2014 г. – 106, в 2015 г. – 119, в 2016 г. – 193 уголовных дела.

Диаметрально противоположная ситуация с выявлением и расследованием уголовных дел, возбужденных по фактам мошенничества, совершенного с использованием компьютерных и телекоммуникационных технологий (с 29.11.2012 – мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). На протяжении последних лет отмечается постоянный рост этой разновидности компьютерных преступлений, при этом в 2016 году возбуждено 995 уголовных дел, что на 43,6 % больше по сравнению с 2015 годом, в суд направлено 237 уголовных дел (рост на 23,4 %) и выявлено 135 лиц, совершивших преступления (рост на 45,2 %).

Нельзя не сказать о латентности данного вида преступлений. По оценкам экспертов, латентность «компьютерных» преступлений в США достигает 80 %, в Великобритании – до 85 %, в ФРГ – 75 %, в России – более 90 %. Также сле-

дует отметить тот факт, что сумма ущерба от преступлений, совершенных в сфере телекоммуникаций и компьютерной информации (если сравнить удельный вес исследуемого состава с иными преступлениями), значительна по отношению к другим видам составов УК РФ.

Что касается источников киберпреступлений, то специалисты подразделяют лиц, осуществляющих атаки, на несколько категорий. Однако между этими категориями не существует достаточно четких границ. Таким образом, деление на группы можно считать в каком-то смысле условным[1].

1. Хакеры – лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций.

Некоторые хакеры не только получают доступ к информации или программному обеспечению, но и перепродают ставшие им доступными сведения.

2. Хактивисты. Термин «хактивизм» возник из соединения двух слов «hack» и «activism» и используется для обозначения явления социального протеста, которое представляет собой своеобразный синтез социальной активности, преследующей цель протеста против чего-либо, и хакерства (использования Интернет-технологий с целью причинения ущерба компьютерным сетям и их пользователям).

3. Киберпреступники (корыстные преступники) – лица, вторгающиеся в информационные системы для получения личных имущественных или неимущественных выгод.

4. Лица, занимающиеся шпионажем, «шпионы», – лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях.

5. Террористы – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политическо-

[1] Яблоков Н. П. Криминалистика: учебник. М.: ЛексЭст, 2006; Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Электронный ресурс. URL: http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb=1&pb=1 (дата обращения –

го воздействия.

6. Вандалы – лица, взламывающие информационные системы для их разрушения.

7. Психически больные лица, страдающие новым видом психических заболеваний, – информационными болезнями или компьютерными фобиями.

Профили киберпреступников:

1. Кодеры – это, квалифицированные программисты, изготавливающие преступные инструменты – программы-вирусы, пользовательские боты, программы для рассылки спама и др.

2. Дропы. Играют важную роль в киберпреступлениях, именно они превращают похищенные логины и PIN-коды в реальные деньги. Работа дропа наиболее опасна: дроп снимает деньги в банкомате и затем передает их заказчику.

3. Подростковая киберпреступность преступность. Киберпреступность, увы, молодая, и ее основанная рабочая сила – подростки в возрасте 15+. Именно они посещают многочисленные чаты, посвященные кардингу и другим подобным темам. Многие подростки пытаются создавать самодельные почтовые программы-мейлеры, создают фишинг-страницы и др.

4. Провайдеры, обслуживающие мошенников. В Интернете организованы AntiAbuseHosting сети («абузоустойчивые» хостинги – на сленге), позволяющие размещать любые противоправные сайты и при этом защищать владельцев этих сайтов от действий правоохранительных органов.

Кроме того, субъекты компьютерных преступлений могут различаться как по уровню их профессиональной подготовки, так и по социальному положению.

Характерные черты киберпреступников. На основании проведенных нами исследований (по данным за 2010-2016 г.г.[1]), можно сделать вывод, что большую часть киберпреступников сосатвляют мужчины в возрасте от 16 до 48

12.02.2017).

лет. Их цели рознятся в зависимости от возраста и социального положения. Если среди молодежи распространены преступления, связанные с нарушением лицензионных соглашений, различных онлайн-проектов (в частности игр) и мелкие мошенничества, то среди более взрослого поколения - такие преступления, как вмешательство в данные, незаконный перехват и т.д.

В настоящее время достижения, полученные в изучении психологии киберпреступников, уже активно применяются в других странах при расследовании преступлений, в основном, при определении типа преступников. Исследования в данной сфере являются также важным теоретическим материалом и могут способствовать развитию изучения психологии девиантного поведения. Как показывает сложившаяся ситуация, в борьбе с киберпреступностью и ее профилактике необходим междисциплинарный подход.

[1] Интернет-ресурс http://www.itsec.ru/main.php (дата обращения – 20.01.2017).

§ 2. Вопросы квалификации мошенничества в сфере компьютерной информации

На стадии выявления преступлений сотрудники подразделений экономической безопасности органов внутренних дел сталкиваются с проблемой предварительной квалификации преступлений, совершаемых с использованием компьютерной информации. Правильное определение состава преступления необходимо для организации работы оперативных сотрудников, в том числе и в рамках дел оперативного учета, определения круга допустимых оперативно-розыскных мероприятий по документированию действий проверяемых лиц[1].

Согласно ст. 159.6 УК РФ под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Основным непосредственным объектом рассматриваемого преступления выступают общественные отношения в сфере охраны собственности. Поскольку данный вид мошенничества характеризуется специфичным способом совершения преступления, а именно вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, то высказываются мнения, что в этом составе дополнительным объектом, который также берется под охрану уголовно-правовой нормой, выступают общественные отношения в сфере защиты компьютерной информации.

Данный вывод предполагает, что при квалификации мошенничества, сопряженного с неправомерным доступом к компьютерной информации, по ст. 159.6 УК РФ не требуется дополнительной квалификации по преступлениям, посягающим на сферу компьютерной информации. Например, в апелляцион-

[1] Об этом подробнее – в 4-м параграфе настоящих методических рекомендаций.

ном постановлении Верховный суд Республики Саха (Якутия) по делу Н., признанному виновным в совершении преступлений, предусмотренных ч. 1 ст. 159.6, ч. 1 ст. 272 УК РФ указал, что диспозиция ст.159.6 УК РФ является специальной по отношению к ст. 159 УК РФ и она полностью охватывает деяния, вмененные подсудимому по данному уголовному делу и соответственно дополнительной квалификации по ст. 272 УК РФ не требуется.[1]

Действительно, согласно правилам квалификации преступлений при конкуренции части и целого, когда деяние предусмотрено двумя или несколькими нормами, одна из которых охватывает содеянное в целом, а другие – его отдельные части, преступление квалифицируется по той норме, которая охватывает с наибольшей полнотой все его фактические признаки. Приведенное правило основано на положении отечественного права, согласно которому виновный должен нести полную ответственность за свои противоправные действия и быть подвергнутым справедливому наказанию.

Однако данное положение не может быть применено в нашем случае, иначе будет нарушен декларированный уголовным законом принцип справедливости. Исходя из понимания данного принципа, мерилом общественной опасности совершенного деяния является вид и размер наказания, определяемые санкцией статьи. Справедливо, что более опасное преступление предусматривает более суровое наказание, а не наоборот.

Включение в конструкцию состава преступления другого самостоятельного преступления, посягающего на иной, дополнительный объект, в отличие от смягчающих наказание обстоятельств, не может понижать общественной опасность деяния, а наоборот, всегда ее повышает, что находит свое отражение в более строгой санкции статьи. Санкция специального состава мошенничества, предусмотренного ст.159.6 УК РФ, содержит менее строгое наказание, чем санкции общего состава мошенничества (ч.1 ст.159 УК РФ) и преступлений в сфере компьютерной информации, совершенных из корыстных побужде-

[1] Постановление по делу № 22-789 // Архив Верховного суда Республики Саха (Якутия).

ний (части 1, 2 ст. 272 и 273 УК РФ). Из этого следует, что преступления в сфере компьютерной информации не могут охватываться составом мошенничества в сфере компьютерной информации и требуют самостоятельной квалификации по совокупности преступлений.

В связи с этим должны остаться в силе (с некоторой корректировкой с учетом изменений уголовного законодательства) разъяснения, данные в постановлении Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», о том, что в случаях, когда мошенничество сопряжено с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статье 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.[1]

Предметом рассматриваемого преступления выступают чужое имущество или право на чужое имущество. Следует отметить, что при мошенничестве в сфере компьютерной информации предметом, как правило, выступает чужое имущество в виде безналичных денежных средств, изъятых у собственника или доверенных им лиц. Случаев получения права на чужое имущество путем манипуляций с компьютерной информацией нами при изучении судебной практики не встречено. Предполагаем, это связано с тем, что даже при наличии развивающегося электронного документооборота получение права на чужое иму-

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 // Бюллетень Верховного Суда РФ. 2008. № 2.

щество в итоге сопряжено с принятием окончательного решения о переходе такого права уполномоченным должностным лицом.

Деяние рассматриваемого преступления выражается в действиях в форме хищения чужого имущества или приобретения права на имущество, осуществляемого в комбинации или одним из следующих способов:

- **ввода компьютерной информации** – размещения сведений в устройствах средств хранения, обработки или передачи компьютерной информации для их последующей обработки и (или) хранения;

- **удаления компьютерной информации** – совершения действий, в результате которых становится невозможным восстановить содержание компьютерной информации и (или) в результате которых уничтожаются носители компьютерной информации;

- **блокирования компьютерной информации** – результата воздействия на компьютерную информацию или технику, последствием которого является ограничение или закрытие доступа к компьютерной информации, связанное с невозможностью в течение некоторого времени или постоянно осуществлять требуемые операции с компьютерной информацией полностью или в требуемом режиме, но не связанных с ее удалением;

- **модификации компьютерной информации** – внесения любых изменений сведений, сообщений, данных, представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами;

- **иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-**

телекоммуникационных сетей – неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного обращения с компьютерной информацией.

Проведенное обобщение судебной практики показывает, что по ст. 159.6 УК РФ квалифицируются хищения чужого имущества, сочетающие в себе комбинацию вышеуказанных способов и, как правило, состоящие в использовании электронных платежных систем (мобильный банк, онлайн-банкинг, банк-клиент и т.д.), вредоносных компьютерных программ.

Так, Октябрьским районным судом г. Томска К. был осужден по ч. 2 ст.159.6 УК РФ. Судом установлено, что К., действуя в группе по предварительному сговору с неустановленным лицом, посредством специальной компьютерной программы (приложения), позволяющей получать удаленный доступ к управлению мобильными телефонами (смартфонами) граждан РФ на базе операционной системы «Android», запущенной в сеть Интернет, и внедренной в устройства сотовой связи, используемые гражданами РФ, не подозревающими о скрытом размещении данной программы, осуществил незаконный доступ к счетам, на которых размещены безналичные денежные средства держателей банковских карт ПАО «Сбербанк России», реквизиты доступа к которым были определены банковским продуктом «Мобильный банк». Затем данная группа **путем ввода, удаления, блокирования, модификации компьютерной информации** совершила хищение безналичных денежных средств граждан РФ на общую сумму 46950 рублей без ведома последних, перечислив денежные средства на банковские карты ПАО «Сбербанк России», находящиеся в пользовании и управлении виновного лица.[1]

Перечислим наиболее часто встречающиеся в следственно-судебной практике **способы мошенничества** в сфере компьютерной информации:

- **хищение путем использования виновным лицом номера телефона потерпевшего, к которому подключена услуга «мобильный банк»; являет-**

[1] Приговор по делу № 1-25/2017 // Архив Октябрьского районного суда г. Томска.

ся наиболее распространенным способом мошенничества в сфере компьютерной информации.

а) потерпевшим в течение нескольких месяцев сим-карта с подключенной услугой «Мобильный банк» не используется, после чего продается компанией сотовой связи новому владельцу, который, получая смс-сообщения с номера 900, имеет возможность осуществлять операции с денежными средствами на счетах потерпевшего.

Например, С. приобрел сим-карту с абонентским номером и с подключенной бывшим владельцем данной сим-карты услугой «Мобильный банк», на которую приходили sms-уведомления о движении денежных средств со счета банковской карты, зарегистрированной на Д. С., достоверно зная, что на счету указанной банковской карты находятся денежные средства в сумме 13 021 рубля, понимая, что имеет доступ к управлению счетом банковской карты, посредством мобильного телефона с использованием услуги «Мобильный банк» путем формирования и отправки sms-сообщения на специальный номер оператора мобильной связи «900» с текстом «5000», то есть ввода компьютерной информации, представленной в форме электрического сигнала, в компьютерную систему банка с последующей модификацией информации о состоянии счета, выраженной в изменении первоначальных данных по движению денежных средств по счету, зачислил со счета указанной банковской карты на счет своего абонентского номера денежные средства в сумме 5 000 рублей, принадлежащие Д. Данные действия квалифицированы судом по ч. 2 ст. 159.6 УК РФ как мошенничество в сфере компьютерной информации с причинением значительного ущерба гражданину.[1]

б) телефон с подключенной услугой «Мобильный банк» выбывает из владения собственника по различным причинам (утрата телефонного аппарата, передача во временное пользование, либо его хищение), и преступник получает

[1] Приговор по делу № 1-64/9-2014// Архив Кировского районного суда г. Курска.

возможность производить манипуляции с денежными средствами, пользуясь данной услугой.

Так, Р., находясь возле торгового отдела, подошла к К. и под вымышленным предлогом, якобы позвонить, попросила у нее сотовый телефон. К., доверяя Р., добровольно передала ей свой сотовый телефон. Затем Р. незаконно внесла изменения в первоначальное состояние данных лицевого счета банковской карты на имя К., выполнив финансовую транзакцию по списанию денежных средств в сумме 5000 рублей с лицевого счета на имя К. и зачислению указанных денежных средств на лицевой счет на имя Р., тем самым похитила денежные средства, принадлежащие К., в сумме 5000 рублей;[1]

в) получение путем использования служебного положения или подложной доверенности дубликата сим-карты с номером, к которому подключена услуга мобильный банк.

Например, К., находясь на своем рабочем месте в офисе продаж и обслуживания ОАО «Вымпелком», используя свое служебное положение, под своей учетной записью осуществила вход в программу АВС «Ensemble» и используя функцию «Запрос данных» осуществила обращение к личной карточке действующего абонента с номером …, принадлежащим Е., после чего с помощью функции замены сим-карты, противоправно, в отсутствие соответствующего заявления клиента Е., произвела замену сим-карты. Убедившись, что на лицевом счете, принадлежащем Е., находятся денежные средства, незаконно осуществила перевод принадлежащих Е. денежных средств с лицевого счета Е. на банковскую карту №, получив реальную возможность распоряжаться поступившими на счет банковской карты денежными средствами;

- **хищение путем получения виновным лицом данных, санкционирующих доступ к банковским счетам (логинов и паролей электронных платежных систем).** Доступ к защищенным ресурсам данных систем может быть осуществлен различными способами:

[1] Приговор по делу № 1-188/2015 // Архив Братского городского суда Иркутской области.

а) получением путем использования вредоносных компьютерных программ и системы удаленного доступа в сети Интернет логинов и паролей, вводимых потерпевшим в зараженный компьютер, посредством которых виновное лицо получает несанкционированный допуск к банковским счетам потерпевшего и управляет движением денежных средств;

б) получением логинов и паролей для доступа к системам электронных платежей благодаря доверительным отношениям с потерпевшим или из информации чеков, оставляемых у банкоматов после активации услуги онлайн-банкинга.

Так, Г. в ночное время отыскивал в мусорных корзинах, стоящих рядом с банкоматами ПАО «Сбербанк России», чек-идентификатор и чек с одноразовыми паролями, используя которые путем удаленного доступа через сеть Интернет с помощью системы дистанционного банковского обслуживания «Сбербанк ОнЛ@йн» незаконно проникал в «личный кабинет» клиента ПАО «Сбербанк России», после чего с помощью электронных поручений осуществлял переводы с этого счета денежных средств на счет имеющейся в его распоряжении банковской карты;

- **хищение путем имитации внесения денежных средств в банкоматы или терминалы самообслуживания.** Это также может осуществляться различными способами:

а) имитация внесения денежных средств в банкоматы или терминалы самообслуживания возможна с помощью вредоносной программы, внедренной в банкоматы и терминалы самообслуживания.

Так, Ш., используя вредоносную программу, внедрял ее через зараженные компьютеры-посредники в терминалы самообслуживания. Программа эмулировала принятие купюроприемником терминала наличных денежных средств без фактического их внесения, создавая фонд безналичных денежных средств, которые впоследствии переводились виновным на банковские счета и обналичивались другими соучастниками преступной группы;

б) имитацией внесения денежных средств в банкоматы или терминалы самообслуживания с помощью поддельных денежных купюр.

Так, Б. с целью хищения чужого имущества путем вмешательства в функционирование средств хранения в информационно телекоммуникационных сетей, внеся в платежный терминал четыре поддельные денежные банкноты номиналом 5 000 рублей каждая, выполнил функции по пополнению счета абонентского номера мобильного телефона, после чего перевел безналичные денежные средства на свой счет;

- **хищение путем использования служебного положения и возможности электронного доступа к счетам организации, в которой работает виновное лицо, или ее клиентов.** Например, Л., работавшая в должности старшего специалиста отдела по работе с корпоративными клиентами, используя автоматизированную систему расчетов «Marti», осуществила операции по переносу денежных средств с лицевых счетов ключевых клиентов на подконтрольные ей лицевые счета на общую сумму 75 373 рубля. Затем Л. провела финансовые корректировки на счетах ключевых клиентов, мотивировав это тем, что был применен неправильный тариф, при этом достоверно зная, что тарификация была произведена корректно;[1]

- **хищение путем использования вредоносных компьютерных программ, внедряемых в мобильные устройства или компьютерные системы, подключенные к электронным банковским сервисам.** С помощью вредоносной программы происходит несанкционированная модификация компьютерной информации, формируются подложные электронные платежные поручения или удаляется файл платежного поручения с заменой на подложный, содержащий реквизиты счета, подконтрольного виновному лицу.

Конечно, арсенал мошенников, совершающих хищения в сфере компьютерной информации, постоянно расширяется и не ограничивается только вышеуказанными способами. Выбор конкретного способа совершения преступле-

[1] Приговор по делу № 1-251/6/2013 // Архив Нижегородского районного суда г. Н.Новгорода.

ния зависит от имеющихся познаний и навыков, технической оснащенности и изощренности преступников. Но, как мы видим, во всех приведенных примерах не встречается обман в качестве способа совершения преступления, несмотря на то, что он выступает обязательным признаком любого мошенничества, что вытекает из его определения, данного в ст.159 УК РФ. В связи с этим среди теоретиков и практиков уголовного права возникли дискуссии относительно квалификации нового состава мошенничества, его места в системе норм Особенной части уголовного права, обязательности для него обмана как конструктивного признака состава преступления.

В начале появления новой нормы, предусматривающей ответственность за мошенничество в сфере компьютерной информации, большинство криминалистов полагало, что данный состав является специальным по отношению к общему составу мошенничества, предусмотренному ст. 159 УК РФ. Специальным, конкретизирующим признаком, по их мнению, являлась сфера реализации мошенничества, в нашем случае – компьютерная сфера. Поскольку мошенничество отличает от других видов хищения чужого имущества способ его совершения – обман или злоупотребление доверием, делался вывод, что обман или злоупотребление доверием должны являться конструктивными признаками специального вида мошенничества. Однако следственно-судебная практика говорила об обратном.

Для уяснения истинного содержания рассматриваемой уголовно-правовой нормы необходимо обратиться к тому времени и тем концепциям, в которых она создавалась и принималась. Так, в пояснительной записке к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) Верховным Судом, инициировавшим данные изменения, указывалось, что подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и соверше-

ния вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество.[1]

Аналогичного содержания комментарий о сущности мошенничества в сфере компьютерной информации дан Верховным Судом Российской Федерации в официальном отзыве на законопроект № 53700-6 «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации», внесенный в Государственную Думу Федерального Собрания Российской Федерации.[2]

Как показало изучение научных комментариев по рассматриваемому вопросу, основной причиной инициирования изменений уголовного законодательства Верховным Судом Российской Федерации послужили вопросы квалификации хищений безналичных денежных средств, совершаемых без обмана, но с использованием компьютерных средств. Если квалифицировать подобные хищения как кражу, то ее предметом могут выступать только наличные денежные средства и для признания преступления оконченным необходимо дождаться обналичивания преступником денежных средств, а они могут и не обналичиваться, использоваться, например, для оплаты услуг и т.п.

Если квалифицировать подобные действия как мошенничество, то обязательным признаком данного состава выступает обман, который в хищениях с использованием компьютерной информации обычно отсутствует. Но здесь предметом преступления могут выступать и безналичные денежные средства, следовательно, момент юридического окончания преступления переносится на момент их поступления на счет виновного лица.

Компромиссным решением данного спорного вопроса стало появление нового вида хищения, который, называясь мошенничеством, к нему имеет от-

---

[1] Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) // Справочная правовая система «Консультант Плюс» (дата обращения 01.06.2017).

[2] Письмо Верховного Суда от 25 мая 2012 г. № 2-ВС-2733/12 // Справочная правовая система «Консультант Плюс» (дата обращения 01.06.2017).

даленное отношение. Предусмотренный ст. 159.6 УК РФ состав никак не связан с общим составом мошенничества (ст. 159 УК РФ) и представляет собой не специальный, а отдельный, новый вид хищения чужого имущества в сфере компьютерной информации, где обман или злоупотребление доверием могут выступать лишь только в качестве факультативных признаков состава преступления. Именно так его и восприняла судебная практика. Конечно, можно поспорить с целесообразностью названия нового вида хищения мошенничеством, но это уже вопрос к законодателю.

Итак, из диспозиции ст. 159.6 УК РФ следует, что способом хищения чужого имущества или приобретения права на имущество выступает не обман или злоупотребление доверием, а ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Если манипулирование компьютерной информацией используется как инструмент обмана, а не завладения чужим имуществом или правом на имущество, то такие действия охватываются традиционной нормой о мошенничестве, т. е. ст. 159 УК РФ. Здесь уместно вспомнить замечание, сделанное Правительством Российской Федерации в официальном отзыве от 02.08.2012 № 3904п-П4 на проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы). В нем было указано, что в соответствии с предложенной редакцией проекта ст. 159.6 УК РФ уголовной ответственности не будут подлежать такие виды компьютерного мошенничества, как мошеннические операции путем выставления счетов за неоказанные услуги (кремминг), ложные предложения товаров и услуг через сеть Интернет с предоплатой, финансовые интернет-аферы (соинвестирование, ложная благотворительность) и др.[1] Правительством РФ было предложено до-

[1] Официальный отзыв от 02.08.2012 № 3904п-П4 на проект Федерального закона «О внесе-

работать законопроект и устранить замечания, но этого законодателем сделано не было.

Помимо указанных Правительством Российской Федерации способов хищения, не подпадающих под состав мошенничества в сфере компьютерной информации, следует отметить так называемые социальные виды мошенничества с использованием информационно-телекоммуникационных сетей, посредством которых мошенник вводит в заблуждение потерпевших относительно различных фактов и просит провести платеж или перевод на закрепленный за ним номер или счет; использование преступником вредоносных программ, блокирующих или шифрующих компьютерную информацию с последующим предъявлением требований о переводе денежных средств как условия отмены блокировки.

Нередко суды не видят отличий между способом обмана потерпевшего и способом совершения хищения и, соответственно, приходят к неверным выводам. Например, приговором Первомайского районного суда Оренбургской области С.О. и С.Е. были осуждены по ч.2 ст. 159.6, ч.2 ст. 273 УК РФ. Суд установил, что эти лица, используя персональный компьютер, создали в сети Интернет сайты, содержащие различную информацию, в стартовый файл которых были заранее интегрированы вредоносные скрипты (программы), которые, внедряясь в чужой компьютер, блокировали его работу. При этом пользователям зараженных компьютеров приходят рассылки якобы от имени МВД России, Управления «К» МВД России, Интерпола, содержащие сведения о необходимости перечисления денежных средств на абонентские номера…, в качестве оплаты наложенного на пользователя сети Интернет административного штрафа за просмотр, хранение и распространение материалов порнографического содержания. В дальнейшем С.Е. и С.О. денежные средства, поступившие

нии изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) // Справочная правовая система «Консультант Плюс» (дата обращения 01.06.2017).

на абонентский номер, перевели на подконтрольный им электронный кошелек.[1]

На наш взгляд, суд в этом примере не учел, что путем манипуляции компьютерной информацией с использованием вредоносной программы преступники лишь создали предпосылки для совершения хищения, вводя в заблуждение потерпевших. Но главная роль, и в этом специфика мошенничества, была уготована потерпевшим, которые посредством использования информационно-телекоммуникационных сетей сами (а не преступники), вводя компьютерную информацию, переводят деньги преступникам, тем самым доводят объективную сторону хищения до его логического завершения. Таким образом, здесь имеет место простое мошенничество, квалифицируемое по ст.159 УК РФ.

Предпосылкой для последующего хищения чужого имущества, а не самим хищением являются также случаи занижения товарной стоимости реализуемого товара посредством модификации данных в программах, обеспечивающих учет и контроль за их движением.

Например, П., работая продавцом в торговой точке, обнаружил на мониторе компьютера открытый файл обновлений программы «1С-Рарус» и, установив, что обновление программы «1С-Рарус» в торговой точке не производилось, умышленно, из корыстных побуждений, с целью хищения имущества изменил в открытом файле обновлений стоимость сотового телефона, удалив установленную стоимость и введя заведомо ложную. Измененный файл П. ввел в программу «1С-Рарус», выполнил обновление программы, в результате чего модифицировал программу «1С-Рарус», получив тем самым возможность реализовать и приобрести для личных целей сотовый телефон по заведомо заниженной цене.[2]

В другом случае П. и Е., работая в ЗАО «…» в должности специалистов офиса продаж, используя свое служебное положение и имея доступ к компьютерной информации, посредством использования служебного компьютера с

---

[1]Приговор по делу № 1-58/ 2016 // Архив Первомайского районного суда Оренбургской области.

[2] Приговор по делу №1-90/2013 // Архив Первомайского районного суда г. Пензы.

установленным на нем программным обеспечением «1С», путем ввода компьютерной информации и замены артикулов дорогостоящей продукции на артикулы менее дорогой продукции, получили возможность похитить указанные товары из офиса продаж и обратить их в своё пользование.[1]

Действия указанных лиц, по нашему мнению, ошибочно квалифицированы судом по ст. 159.6 УК РФ как мошенничество в сфере компьютерной информации, поскольку подтасовка цены, артикулов товара является лишь предпосылкой для его последующего хищения путем осуществления договора купли-продажи товара по заниженной цене.[2]

В других случаях судами ошибочно квалифицируются как мошенничество в сфере компьютерной информации действия, связанные с манипуляцией компьютерной информацией, скрывающей следы совершенного хищения. Так, П., работая в должности старшего бухгалтера расчетной группы филиала..., составила платежную ведомость, в которую незаконно внесла свою фамилию и указала сумму в размере 3 035 рублей к выплате из кассы филиала, которая ей не полагалась. В этот же день на основании указанной ведомости П. получила в кассе филиала деньги в указанной сумме. Затем П., имея непосредственный доступ к начислению и удержанию денежных средств работникам филиала и используя свое служебное положение, применив личный пароль доступа к информационно-аналитической базе, установленной на ее служебном компьютере, внесла недостоверные исправления в платежную ведомость, введя в нее фамилию и сумму подотчета 3 035 рублей. После этого программа информационно-аналитической базы автоматически отразила в карточке сотрудника и в его расчетном листке сумму 3 035 рублей в качестве выданного ему подотчета, тем самым образовав у последнего долг перед филиалом, с причинением материального ущерба на указанную сумму.[3]

Представляется неверным квалифицировать вышеуказанные действия

---

[1] Приговор по делу №1-176/2013 // Архив Пресненского районного суда г. Москвы.
[2] Приговор по делу № 1-64/9-2014г. // Архив Кировского районного суда г. Курска.
[3] Постановление по делу № 1-242/2013 // Архив Енисейского районного суда Красноярского

как мошенничество в сфере компьютерной информации, поскольку в них хищение чужого имущества совершено путем подлога официального документа. Действия П. следует оценивать как мошенничество, совершенное лицом с использованием своего служебного положения по ч. 3 ст. 159 УК РФ. Данное преступление юридически окончено с момента получения обманным путем денежных средств из кассы, поскольку с этого времени П. получает возможность распоряжаться ими по своему усмотрению. Поэтому манипулирование П. компьютерной информацией выходит за рамки состава преступления и должно быть квалифицировано как сокрытие следов совершенного преступления.

Не могут быть квалифицированы как мошенничество в сфере компьютерной информации действия, связанные с незаконным получением услуг имущественного характера. Так, приговором мирового судьи судебного участка № 3 Центрального района г. Читы был осужден Ф. по ч. 1 ст. 159.6 УК РФ. Судом установлено, что Ф., являясь специалистом по обслуживанию в Контактном центре ОАО «Мегафон», путем модификации компьютерной информации изменил в программе «SBMS» категорию клиента с «Коммерческой» на «Технологическую» на принадлежащем ему абонентском номере с целью безвозмездного пользования услугами связи (интернет). Таким образом с 29.11.2013 по 30.11.2013 Фадеев, продолжая реализацию своего преступного умысла, похитил денежные средства в сумме 7 85694 рубля путем использования услуг связи (интернет) в личных целях. Своими действиями Фадеев причинил ОАО «Мегафон» материальный ущерб на сумму 7 85694 рубля.

В приведенном случае предметом преступления выступили не имущество и не право на чужое имущество, а услуги имущественного характера. Следовательно, данные действия необходимо было квалифицировать по ст.165 УК РФ как причинение имущественного ущерба путем обмана или злоупотребления доверием без признаков хищения. Поскольку в данном составе преступления обязательным признаком выступают общественно опасные последствия в виде

края.

ущерба в крупном размере (ущерб, превышающий 250 тысяч рублей), а данный признак в содеянном Ф. отсутствует, его действия подпадают под признаки не уголовного, а административного правонарушения, предусмотренного ст.7.27.1 КоАП РФ. Помимо неправильной квалификации, следственными органами не дана оценка совершенному Ф. неправомерному доступу к компьютерной информации, совершенному из корыстных побуждений, квалифицируемому по ч. 2 ст. 272 УК РФ.

Более сложным для квалификации представляется деяние, совершенное Ф., который был осужден Пролетарским районным судом г. Твери по ч. 2 ст. 272, ч. 1 ст. 159.6 УК РФ. Судом установлено, что Ф., являясь специалистом группы оперативного обслуживания клиентов и имея индивидуальный и конфиденциальный логин и пароль, получил доступ к базе данных, содержащей персональные данные клиентов ОАО…, активировал компьютерную программу CRM, после чего ввел в поисковую строку данного модуля свой абонентский номер, получив доступ к личной карточке абонента, затем открыл программу ССВО, предназначенную для осуществления корректировок и просмотра сведений о детализации абонентского номера, открыл вкладку «корректировки», и, осознавая, что не имеет права самостоятельно производить корректировки баланса счета своего абонентского номера, произвел корректировку (изменение) баланса счета абонентского номера №, зарегистрированного на его имя, увеличив баланс счета на общую сумму … рублей. Таким образом осознавая, что денежные средства ОАО … ему не принадлежат и он не имеет права ими распоряжаться, похитил денежные средства в размере … со счета ОАО … .[1]

Представляется, что в этом случае квалификация деяния зависит от того, какой статус имели виртуальные расчетные единицы, используемые компанией. Если только как средство оплаты за оказанные услуги сотовой связи, то такие действия необходимо квалифицировать, при наличии крупного ущерба, по

[1] Приговор по делу № 1-210/15 // Архив Пролетарского районного суда г. Твери.

ч. 1 ст. 165 УК РФ и ч. 2 ст. 272 УК РФ. Если виртуальные расчетные единицы компании могут быть конвертированы в безналичные денежные средства и затем обналичены или использоваться на покупку товаров, оплату услуг ЖКХ и т.п., то такие действия правильно квалифицировать по ст.159.6 УК РФ и ч. 2 ст. 272 УК РФ.

Согласно п. 4 постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество признается оконченным с момента, когда имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность (в зависимости от потребительских свойств этого имущества) пользоваться или распорядиться им по своему усмотрению.

Если мошенничество совершено в форме приобретения права на чужое имущество, преступление считается оконченным с момента возникновения у виновного юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом как своим собственным.

При мошенничестве, совершенном путем перевода безналичных денежных средств, преступление следует считать оконченным с момента зачисления этих средств на счет лица, которое путем обмана или злоупотребления доверием изъяло денежные средства со счета их владельца, либо на счета других лиц, на которые похищенные средства поступили в результате преступных действий виновного.[1]

Непростым является вопрос о признании преступления оконченным и квалификации мошенничества в сфере компьютерной информации как единого продолжаемого преступления, если лицо несколько раз совершило действия, содержащие признаки, указанные в статье 159.6 УК РФ.

Согласно разъяснениям, данным в постановлении Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 24.05.2016) «О судебной практике по де-

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 // Бюллетень Верховного Суда Российской Федерации. 2008. № 2.

лам о краже, грабеже и разбое», от совокупности преступлений следует отличать продолжаемое хищение, состоящее из ряда тождественных преступных действий, совершаемых путем изъятия чужого имущества из одного и того же источника, объединенных единым умыслом и составляющих в своей совокупности единое преступление.

Таким образом, для признания мошенничества в сфере компьютерной информации единым продолжаемым преступлением, необходимо установить совокупность признаков:

- хищение характеризуется совершением ряда тождественных действий;
- эти тождественные действия объединены единым преступным умыслом, возникшим единовременно;
- хищение совершается из одного источника.

Продолжаемое преступление признается оконченным с момента совершения последнего из ряда тождественных действий, направленных на реализацию преступного умысла.

Как представляется, совокупность преступлений при совершении мошеннических действий в сфере информационных технологий отсутствует в случаях, когда многоэпизодный характер изъятия имущества обусловлен установленными ограничениями по переводу денежных средств.

В то же время имеется совокупность преступлений в случаях, когда умысел на изъятие имущества формируется у лица каждый раз заново на основе получения информации о поступлении на расчетный счет денежных средств. Однако если лицо изначально стремилось незаметно для потерпевшего продолжительное время изымать денежные средства путем перечисления незначительных сумм (например, по 100 – 200 руб.), то такие действия необходимо квалифицировать как единое продолжаемое преступление.

Единым продолжаемым преступлением также следует признавать случаи совершения лицом компьютерного мошенничества способами, предполагающими автоматическое срабатывание вредоносного программного обеспечения,

в результате которого происходит изъятие денежных средств потерпевших, при этом виновное лицо может и не знать определенно, сколько граждан пострадает в результате его преступных действий. [1]

С субъективной стороны мошенничество в сфере компьютерной информации характеризуется наличием у виновного прямого умысла, направленного на хищение чужого имущества или на приобретение права на чужое имущество. При совершении этого преступления виновный не только сознает общественно опасный характер своих действий и предвидит причинение общественно опасных последствий в виде реального имущественного ущерба собственнику (владельцу) имущества, но и желает путем совершения таких действий обратить в свою собственность похищенное имущество (право на него) за счет причинения ущерба законному собственнику (владельцу) имущества.

Поскольку необходимый признак мошенничества – отсутствие у виновного права на имущество, это обстоятельство также входит в содержание интеллектуального момента умысла. Совершая мошенничество, субъект сознает, что это имущество ему не принадлежит. Отсутствие такого сознания исключает возможность квалификации деяния как мошенничества (при определенных условиях речь может идти о самоуправстве).[1]

Содержание субъективной стороны рассматриваемого преступления не исчерпывается умыслом. В нее также входит в качестве обязательного элемента корыстная цель, которая представляет собой желаемый для виновного результат, – получение фактической возможности владеть, пользоваться (удовлетворять личные материальные потребности) и распоряжаться чужим имуществом как своим собственным (продать, подарить или на иных основаниях передать другим лицам).

Установление прямого умысла и корыстной цели – необходимые условия для привлечения к ответственности за мошенничество, так как мошенниче-

[1] Фролов М.Д. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Адвокат. 2016. № 6. С. 53 - 58.

ство является формой хищения, а в определении хищения законодатель закрепил обязательное наличие корыстной цели при совершении любого хищения. Отсутствие корыстной цели свидетельствует об отсутствии состава мошенничества.[2]

Признаки состава преступления, характеризующие субъекта, немногочисленны. Субъектом мошеннического посягательства, как и любого преступления, может быть только физическое вменяемое лицо, достигшее установленного уголовным законом возраста. Мошенники в сфере компьютерной информации, как правило, обладают определенными профессиональными знаниями в банковском деле, бухгалтерии, в области компьютерных технологий и т.п. В подавляющем большинстве случаев мошенники действуют одним и тем же способом. Зачастую мошенники совершают преступление группами, обязанности членов которых заранее распределены и исполняются с высокой точностью и преступным профессионализмом. Уголовной ответственности за мошенническое посягательство подлежат лица, достигшие ко времени совершения преступления шестнадцатилетнего возраста.

Действующее уголовное законодательство, определяя понятие мошеннического посягательства, предусматривает ряд обстоятельств, при наличии которых рассматриваемое преступление признается более опасным для общества. Эти обстоятельства учтены законодателем в качестве квалифицирующих признаков мошеннического посягательства.

К квалифицированному виду мошеннического посягательства, предусмотренного ч. 2 ст. 159 УК России, относится мошенничество, совершенное:

а) группой лиц по предварительному сговору;

б) с причинением значительного ущерба гражданину.

---

[1] Кочкина С.В. Субъективная сторона мошенничества.// Вестник Барнаульского юридического института МВД России. 2006. № 10. С. 18.

[2] Выявление и раскрытие мошенничества : учеб.пособие / под общ.ред. В.П. Сальникова. С-Пб: Лань, 2000. С. 64.

Часть 3 ст. 159 УК России говорит о более опасных для общества квалифицированных видах мошенничества, совершенных:

а) лицом с использованием своего служебного положения;

б) в крупном размере.

Часть 4 ст. 159 УК России говорит о еще более опасных для общества квалифицированных видах мошенничества, совершенных:

а) организованной группой;

б) в особо крупном размере.

Мошенничество признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении этого преступления. Предварительным считается сговор, состоявшийся до начала мошенничества, во время приготовления к нему или непосредственно перед покушением. Промежуток времени между сговором и началом мошеннического посягательства не имеет значения. Присоединение лица к уже начатому мошенничеству с последующим сговором о совместном окончании преступления не дает основания усматривать здесь данный квалифицирующий признак.

По признаку группы с предварительным сговором могут квалифицироваться действия также тех лиц, которые непосредственно участвовали в совершении мошеннического посягательства как соисполнители преступления. При этом необязательно, чтобы все они выполняли одинаковые действия. Действия соисполнителей квалифицируются без ссылки на ст. 33 УК России. Действия лиц, которые непосредственно не участвовали в совершении мошенничества, а ограничились подстрекательством или обещанием скрыть похищенное, или иным путем содействовать мошеннику, должны квалифицироваться по ч. 4 и ч. 5 ст. 33 и ст.159 УК России.

Особенность соучастия в компьютерном мошенничестве состоит в том, что соучастники взаимодействуют не в реальной, а в виртуальной среде ди-

станционно и зачастую анонимно. В связи с этим возникает вопрос относительно юридической оценки действий лица, которое, например, на специальном форуме распространяет сведения о способах совершения компьютерного мошенничества, предоставляет возможность приобретения соответствующего программного обеспечения (легального или вредоносного), специального оборудования (например, скиммеров), реквизитов банковских карт и банковских счетов, отсканированных копий.

С точки зрения института соучастия, сложившегося в теории уголовного права России, содеянное такими лицами не образует соучастия в форме пособничества, даже при том условии, что такое лицо осознает, что оно тем самым способствует совершению другими лицами преступлений (однако лишь абстрактно). [1]

Мошенничество признается совершенным с использованием виновным своего служебного положения в случае, если для изъятия и (или) обращения чужого имущества либо приобретения права на него субъектом была использована занимаемая им должность в любых учреждениях или организациях независимо от формы собственности. При этом не имеет значения, является ли виновный должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации.[1]

Мошенничество, совершенное с причинением значительного ущерба гражданину, может иметь место при посягательствах на частную собственность каждого лица в отдельности. Например, значительным ущербом для гражданина может признаваться ущерб, равный сумме, которую гражданин не может покрыть за месячную заработную плату, а также учитывается финансовое положение семьи потерпевшего, но не менее 2500 рублей. В этом состоит особенность данного квалифицирующего признака по сравнению с другими, установление которых не зависит от формы собственности.

---

[1] Фролов М.Д. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Адвокат. 2016. № 6. С. 53-58.

Мошенничество признается совершенным организованной группой, если оно «совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений» (ст. 35 УК России). Отличительным признаком данной группы является устойчивость, которая обычно предполагает умысел соучастников на совершение не одного, а нескольких преступлений. Устойчивой группа может быть признана даже при совершении одного преступления, когда оно требовало длительного времени подготовки, исполнения, плотного взаимодействия между соучастниками, действовавшими в одном составе. Факультативными признаками, указывающими на устойчивость группы, являются наличие руководителей, предварительная подготовка преступных деяний, подбор соучастников и распределение ролей между ними, обеспечение мер по сокрытию преступлений, наличие отработанных методов преступной деятельности.

Согласно ч. «б» ст. 35 УК России создание организованной группы в случаях, специально не предусмотренных Особенной частью УК России, влечет ответственность за приготовление к тем преступлениям, для совершения которых она создана. В соответствии с ч. 5 ст. 35 УК России лица, создавшие организованную группу или преступное сообщество либо руководившие ими, подлежат ответственности за их организацию и руководство в случаях, предусмотренных Особенной частью УК России, а также за все совершенные организованной группой или преступным сообществом преступления, если они охватывались их умыслом. Другие участники организованной группы или преступного сообщества несут ответственность за участие в них в случаях, предусмотренных Особенной частью УК России, а также за преступления, в подготовке или совершении которых они участвовали.[1]

Мошенничество признается совершенным в крупном размере в случае, если стоимость похищенного имущества превышает 1000 000 рублей.

---

[1] Михаль О.В. Сложности квалификации мошенничества.// Уголовное право. 2009. № 6. С. 34.

Совершение нескольких хищений чужого имущества путем обмана или злоупотребления доверием, образующих в общей сложности крупный размер, если содеянное свидетельствует о едином продолжаемом преступлении (все мошеннические действия совершены одним способом и при обстоятельствах, свидетельствующих об умысле совершить хищение в крупных размерах), надлежит квалифицировать как хищение в крупном размере.

Говоря о совершении мошенничества в крупных размерах, следует отметить, что при совершении мошенничества группой лиц размер хищения определяется общей стоимостью похищенного имущества без учета фактически полученной доли каждым из соучастников. Если же отдельные соучастники принимали участие не во всех эпизодах хищения, то квалификация их действий должна зависеть от размера ущерба, причиненного теми преступлениями, в которых они участвовали.

---

[1] Ледяев А.П. Классификация криминалистически значимых признаков организованного мошенничества// Российский судья. 2011. № 9. С. 28.

ГЛАВА 2. РАСКЫТИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Организация деятельности подразделений ЭБиПК по выявлению преступлений, предусмотренных ст. 159.6 УК РФ

Борьба с хищениями, совершаемыми с использованием компьютерной информации, невозможна без осуществления оперативно-розыскной деятельности (ОРД), поскольку применение исключительно уголовно-процессуальных и административно-правовых мер не позволяет выявлять, раскрывать и предупреждать эти преступления. В государственно-правовой функции борьбы с преступностью оперативно-розыскная деятельность занимает особое место, обусловленное ее уникальными разведывательно-поисковыми возможностями. Об этом свидетельствуют и данные проведенного нами исследования – подавляющее число преступлений по ст. 159.6 УК РФ раскрываются с использованием оперативно-розыскных сведений. Вместе с тем эффективность оперативно-розыскной деятельности зависит от умелой ее организации.

Рассматривая сущность организации оперативно-розыскной деятельности органов внутренних дел (ОВД) по борьбе с мошенничеством в сфере компьютерной информации, обратимся к базовым элементам, отражающим в целом содержание организации оперативно-розыскной деятельности органов внутренних дел.

Обобщив различные научные источники, следует констатировать, что организация может рассматриваться в двух аспектах: как *«организация системы управления»* и *«организация процессов управления».* При этом специалистами теории управления в содержание «организации системы» включаются следующие основные элементы: определение целей; постановка задач; определение функций для достижения поставленных целей; разработка организационно-штатных структур; подбор кадров (разработка качественной и количественной модели); информационное, аналитическое, методическое обеспечение и др.

В теории *организацию процессов управления* традиционно подразделяют на два основных блока: *процесс принятия управленческого решения* и *процесс исполнения управленческого решения.*

При этом специалисты теории управления в первый блок включают следующие основные элементы: анализ оперативной обстановки, прогнозирование, планирование, подготовку управленческого решения (приказа, распоряжения) и др. В содержание *«процесса исполнения управленческого решения*» учеными включаются такие элементы, как: доведение решения до исполнителей, инструктаж, расстановка сил и средств, материально-техническое обеспечение, взаимодействие, координация, контроль, учет, коррегирование и др[1].

Анализ различных позиций авторов показывает, что до настоящего времени в теории не сложилось единого мнения о содержании, объеме и последовательности отдельных элементов организации. Многие специалисты предлагают свои модели и классификации. Например, согласно одному из вариантов, выполнение функции организации предполагает: формирование функциональной и организационной структур, обоснование штатной численности, подбор и расстановку кадров, информационное, материально-техническое и финансовое обеспечение, установление между всеми элементами исполнительной деятельности устойчивой взаимосвязи, гарантирующей их надежное взаимодействие[2].

Не останавливаясь на детальной оценке приведенных подходов к понятию организации ОРД, полагаем, что, несмотря на определенные особенности, все они достаточно обоснованы и позволяют подойти к пониманию ее сущности. Вместе с тем понятие «организация ОРД ОВД» должно быть сформулировано наиболее емко и предметно. Современное понимание сущности рассматриваемой категории дает следующее определение: «*Организация оперативно-розыскной деятельности органов внутренних дел представляет собой ком-*

---

[1] См.: Попова А.М. Процесс управления в сфере правоохранительной деятельности // Теория управления в сфере правоохранительной деятельности: учебник. М., 1990. С. 137, 168-171; Туманов Г.А. Организация управления в сфере охраны общественного порядка. М., 1972. С. 168-173.

[2] Основы управления в органах внутренних дел: учебник. М., 2002. С. 60.

плекс (систему) специальных организационных мер, используемых руководителями органов внутренних дел, их оперативных подразделений и иными субъектами в целях эффективного применения оперативно-розыскных сил, мероприятий, методов, форм и средств для решения задач оперативно-розыскной деятельности»[1].

Как следует из определения, первый из базовых элементов организации ОРД ОВД связан с применением *комплекса (системы) специальных организационных мер*. Именно этот элемент мы рассмотрим в рамках данных методических рекомендаций.

Согласно подходу, развивавшемуся с начала становления науки об организации[2], ее содержание раскрывается в двух основных значениях: как состояние любой системы, предназначенной для решения конкретных задач в определенной форме; как функция управления, т.е. деятельность, приводящая систему в целенаправленное «движение»[3]. Первое значение определяет статику системы, ее состояние на определенный период[4]. Нередко в литературе их называют функциями-задачами. Второе значение – составная часть процесса управления характеризует ее в динамике, функционировании, «движении». В научной литературе их зачастую называют функциями-операциями[5], которые, по своей сути, образуют организационно-управленческие меры.

Такой подход сочетается с предлагаемым нами содержанием организации ОРД, которое включает в себя основные «статические» и «динамические» меры (функции). Применительно к борьбе с мошенничеством в сфере компью-

---

[1] Атмажитов В. М., Музеев А.И. Некоторые аспекты определения сущности организации оперативно-розыскной деятельности органов внутренних дел по борьбе с бандитизмом // Вестник Казанского ЮИ. Казань: КЮИ МВД России, 2012. № 1. С. 71.

[2] См. напр.: Богданов А. А. Очерки организационной науки. М., 1922. URL: http://www.uic.unn.ru/pustyn/lib/bogdanov.ru.html (дата обращения - 17.01.2017).

[3] Саввинов А. Г. Методика анализа и оценки управленческой деятельности: лекция. М., 1996. С. 4; Акимова Т. А. Теория организации: учебное пособие для вузов. М., 2003. С. 11; Теория организации: учебник / под общ. ред. Г. В. Атаманчука. М., 2007. С. 32-33.

[4] Токарев Е. В. Основы организации оперативно-розыскной деятельности органов внутренних дел и пути ее совершенствования: лекция. М., 1994. С. 15-16.

[5] Туманов Г. А. Организация управления в сфере охраны общественного порядка. М., 1972. С. 138, 166.

терной информации они представлены следующим образом:

- научно обоснованное определение приоритетных направлений борьбы с кибермошенничеством, а также четкая постановка объективно необходимых и реально достижимых целей и задач подразделениями органов внутренних дел, осуществляющими деятельность по выявлению, предупреждению и раскрытию преступлений, совершаемых с использованием компьютерной информации;

- осуществление нормотворческой (нормопроектирующей) работы с целью совершенствования ОРД по борьбе с мошенничеством в сфере компьютерной информации;

- разработка и совершенствование организационно-структурного обеспечения подразделений ОВД с учетом реализации функции борьбы с преступлениями, совершаемыми с использованием высоких технологий;

- создание эффективной системы информационного и аналитического обеспечения деятельности подразделений органов внутренних дел в решении ими задач по борьбе с мошенничеством в сфере компьютерной информации;

- прогнозирование и планирование ОРД ОВД по борьбе с мошенничеством в сфере компьютерной информации;

- организация внешнего и внутреннего взаимодействия субъектов борьбы с киберпреступностью;

- создание действенной и эффективной системы контроля за деятельностью подразделений ОВД, осуществляющих борьбу с киберпреступностью;

- оценка состояния борьбы с преступлениями, совершаемыми с использованием высоких технологий, разработка и внедрение стимулирующих ее критериев и показателей;

- оказание практической помощи территориальным подразделениям ОВД по выявлению лиц, совершающих преступления с использованием компьютерной информации, пресечение и документирование их противоправной деятельности;

- управление кадрами специализированных подразделений экономиче-

ской безопасности и специальных технических мероприятий, в чьи функции входит борьба с преступлениями, совершаемыми с использованием высоких технологий;

- подготовка сил и средств ОВД к действиям в условиях чрезвычайных обстоятельств, связанных с деятельностью организованных преступных структур, совершающих преступления в сфере компьютерной информации.

Проведенное нами исследование позволило сформулировать определение организации оперативно-розыскной деятельности по борьбе с преступлениями, совершаемыми с использованием компьютерной информации, под которой мы понимаем *комплекс (систему) специальных организационных мер, осуществляемых руководителями органов внутренних дел, оперативных подразделений и иными субъектами в целях эффективного применения ими оперативно-розыскных сил, мероприятий, средств и форм по установлению лиц, использующих компьютерную информацию для подготовки и совершения преступления, а также его своевременного выявления и раскрытия.*

Организация ОРД ОВД по борьбе с преступлениями с использованием высоких технологий основывается на тесном сочетании организационно-управленческих и организационно-тактических мер, которые обеспечивают единство системы, ее постоянное совершенствование, а также адекватное реагирование на динамичные изменения оперативной обстановки.

Среди ключевых проблем организации ОРД выделяется разграничение компетенции между оперативными подразделениями органов внутренних дел по обеспечению расследования уголовных дел по преступлениям, совершенным с использованием информационных технологий.

Указанная проблема, в частности, рассматривалась на Коллегии МВД по Республике Татарстан от 27 марта 2015 года № 2 КМ «О проблемных вопросах организации работы по раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий и коммуникаций». По итогам Коллегии министром внутренних дел по Республике Татарстан издано распоряжение от 17.04.2015 № 83-р, согласно которому:

1) к компетенции подразделений специально-технических мероприятий (далее ПСТМ) МВД по Республике Татарстан отнесено раскрытие мошенничества, совершенного в совокупности с неправомерным доступом к компьютерной информации и (или) созданием, использованием, распространением вредоносных компьютерных программ (ст.159.6 УК РФ, ст.159 УК РФ в совокупности со ст. 272 УК РФ и (или) ст. 273 УК РФ);

2) преступления, совершенные с использованием современных информационных технологий и коммуникаций, состав которых образуют хищения чужого имущества или приобретение права на чужое имущество путем мошенничества, входят в компетенцию управления экономической безопасности и противодействия коррупции (далее УЭБиПК) только при наличии, в совокупности, следующих условий:

– при совершении преступления использовались реквизиты юридического лица или гражданина, осуществляющего предпринимательскую деятельность без образования юридического лица;

– при совершении преступления использовался счет кредитной организации, открытый от имени юридического лица или гражданина, осуществляющего предпринимательскую деятельность без образования юридического лица;

– количество потерпевших в результате совершения преступления составляет десять и более лиц.

3) к компетенции Управления уголовного розыска МВД по Республике Татарстан отнесены преступления, совершенные с использованием современных информационных технологий и коммуникаций, состав которых образуют хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, то есть мошенничество (ст. 159 УК РФ) общеуголовного характера.[1]

Вопросы, связанные с раскрытием преступлений, а также рассмотрением материалов проверок по заявлениям и сообщениям о правонарушениях

[1] Здесь сохранены формулировки, использованные в распоряжении министра внутренних дел

(преступлениях) компетенции ПСТМ, принято решать посредством направления письменных запросов в подразделение «К» ПСТМ при МВД по Республике Татарстан.

Полагаем, что приведенный подход в разграничении компетенции оперативных подразделений и их взаимодействия может быть принят на вооружение и в других территориальных органах МВД России.

§ 2. Документирование преступлений, предусмотренных ст. 159.6 УК РФ

В соответствии с п. 3 ст. 20 УПК РФ[1] уголовные дела по ст. 159.6 УК РФ отнесены к делам частно-публичного обвинения, если они совершены индивидуальным предпринимателем в связи с осуществлением им предпринимательской деятельности и (или) управлением принадлежащим ему имуществом, используемым в целях предпринимательской деятельности, либо если эти преступления совершены членом органа управления коммерческой организации в связи с осуществлением им полномочий по управлению организацией либо в связи с осуществлением коммерческой организацией предпринимательской или иной экономической деятельности. Исключение составляют случаи, когда преступлением причинен вред интересам государственного или муниципального унитарного предприятия, государственной корпорации, государственной компании, коммерческой организации с участием в уставном (складочном) капитале (паевом фонде) государства или муниципального образования, либо если предметом преступления явилось государственное или муниципальное имущество.

Согласно полученным оценкам оперативных работников, следственными органами возбуждаются уголовные дела не более чем в 5 % случаев обращений о хищениях денежных средств с банковских счетов или из электронных ко-

---

по Республике Татарстан от 17.04.2015 № 83-р.

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ.

шельков. Однако, по мнению оперативников, и сами заявления подавались не более чем в половине случаев хищений денежных средств со счетов юридических лиц и не более чем в 1 из 3-5 случаев хищений денежных средств со счетов физических лиц.

Зачастую при обращении потерпевшего в правоохранительные органы по факту хищения в заявлении сообщается только о несанкционированном переводе денежных средств на неизвестный потерпевшему счет (или счета). Поскольку такие преступления происходят в условиях почти полной неочевидности, факт несанкционированного доступа к электронным средствам платежа на момент обнаружения хищения, как правило, не может быть подтвержден. В случае успешного совершения хищения и применения злоумышленником достаточных средств и методов удаления или сокрытия следов это событие однозначно выглядит как преступление только с точки зрения бывшего владельца похищенных средств. Причем сам владелец денежных средств обычно не понимает, каким именно способом совершено преступление.[1]

Отсутствие осведомленности и правильного оперативно-тактического определения ситуации, а также выработанного унифицированного подхода к проведению комплекса первоначальных проверочных мероприятий приводит к ошибочному выбору тактики раскрытия, выполнению тех или иных безрезультатных действий и, следовательно, к затягиванию процессуальных сроков рассмотрения сообщений о преступлениях. Во многих случаях факт совершения хищения с использованием именно вредоносных компьютерных программ так и остается неизвестным как для сотрудников правоохранительных органов, так и для самих владельцев денежных средств, что исключает возможность установления и привлечения всех виновных лиц к уголовной ответственности.[2]

---

[1] Дуленко В.А., Р.Р. Мамлеев, В.А. Пестриков. Преступление в сфере высоких технологий: учебное пособие. М.: ЦОКР МВД России, 2010. С. 20-21.

[2] Шмонин А.В. Методическое обеспечение организации выявления, раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания. // Расследование преступлений: проблемы и пути их решения. М.: Московская академия Следственного комитета Российской Федерации, 2014. № 6. С. 314.

Основные доказательства использования вредоносной программы, а также ввода, удаления, блокирования, модификации компьютерной информации находятся на компьютере или мобильном устройстве потерпевшего. Подтвердить указанные факты можно только в результате сложного технического исследования, которое провести на этапе проверки сообщения о преступлении весьма затруднительно.

Так, в подразделение «К» ПСТМ поступила информация о появлении на территории Российской Федерации нового вида вредоносного программного обеспечения – «Faketoken.b-ruStels2», целью которого являются устройства, работающие на платформе «Android».

В результате проведенных оперативно-розыскных мероприятий установлена организованная группа, в которую входило семь человек. Программу, которую они использовали, после установки на устройство запрашивала баланс привязанной к номеру банковской карты, скрывала поступающие уведомления и начинала осуществлять переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.

В результате проведенных обысков было изъято значительное количество компьютерной техники со следами распространения в сети Интернет вредоносного программного обеспечения, 25 мобильных телефонов, более 150 сим-карт, электронные носители информации и свыше 100 банковских карт, на которые производилось зачисление похищенных денежных средств. Участники преступной группы были задержаны и дали признательные показания. Сумма предотвращенного ущерба клиентам банка по предварительным оценкам составляет более 5 млн руб.

Как показывает практика, не меньшее усердие в уничтожении следов совершения преступлений предпринимают и сами пострадавшие. По наблюдениям опрошенных сотрудников оперативно-розыскных подразделений, до половины пострадавших непосредственно сразу после выявления фактов хищений денежных средств (что часто сопровождается выведением из строя компьюте-

ров) самостоятельно или силами сторонних специалистов производят восстановление вышедших из строя компьютеров, их проверку антивирусными программами (с обязательным удалением найденных вредоносных программ). Иногда – полную замену операционных систем, в том числе с переустановкой платежного программного обеспечения (если таковое имеется), и даже замену носителей информации. После этого уже следуют обращения в правоохранительные органы.

В результате при рассмотрении заявлений по фактам совершенных хищений денежных средств правоохранительные органы в большинстве случаев не имеют подтверждений применения вредоносных компьютерных программ и несанкционированного доступа к электронным средствам платежа или их утраты, а, следовательно, и того, что вообще имел место неправомерный и несанкционированный перевод денежных средств. Предположение о том, что лицо, обратившееся по факту несанкционированного перевода денежных средств, таким способом на самом деле пытается отказаться от собственного легального перевода по каким-либо субъективным причинам, часто является основанием для принятия решения об отказе в возбуждении уголовного дела.

Следовательно, эффективная фиксация фактов противоправной деятельности, связанной с мошенничеством с использованием компьютерной информации, зачастую возможна только в рамках оперативного документирования.

Однако даже если доводы пострадавшего и установленные обстоятельства происшествия оказываются достаточными для принятия решения о возбуждении уголовного дела, возникает проблема квалификации деяния.

Актуальность верной сыскной квалификации криминальных действий обусловлена случаями, когда принимается решение о проведении оперативно-технических мероприятий, связанных с ограничением конституционных прав граждан. Следует иметь в виду, что подобные оперативно-розыскные мероприятия допустимо проводить лишь при условии, что в действиях злоумышленников содержится квалифицированный состав преступления по ст. 159.6 УК РФ. Это следует из положения п. 1 ч. 2 ст. 8 Федерального закона «Об оперативно-

розыскной деятельности»[1], согласно которому проведение оперативно-розыскных мероприятий (включая получение компьютерной информации), которые ограничивают конституционные права человека и гражданина, допускается на основании судебного решения и при наличии информации о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно. Очевидно, что речь идет о тех преступлениях, по которым расследование проводится в форме предварительного следствия, а согласно УПК РФ уголовные дела по ч. 1 ст. 159.6 УК РФ расследуются в форме дознания.[2]

В настоящее время использование различных компьютерных устройств представляет собой и «место» совершения преступлений (например, интернет-ресурсы), и средство их совершения (например, компьютер, ноутбук, планшет и др.). Именно поэтому обеспечение безопасности граждан и государства невозможно без постоянно осуществляемого правоохранительными органами в рамках оперативно-розыскной деятельности добывания информации о действиях криминальных структур и элементов. При этом заметим, что в современном мире значительные объемы такой информации циркулируют в сети Интернет, концентрируются в информационных ресурсах и различных технических устройствах в компьютерной форме.

В оперативно-розыскной науке и практике ведется активный поиск оптимальных форм и методов сбора компьютерной информации. При этом, как правило, отмечается недостаточная правовая регламентация получения доступа к компьютерным данным в интересах оперативно-розыскной деятельности.[3]

С учетом сказанного представляется крайне актуальным дать практические рекомендации по определению сущности и содержания нового оперативно-розыскного мероприятия – «Получение компьютерной информации».

---

[1] Об оперативно-розыскной деятельности: Федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ.

[2] См. п. 3 ст. 150 УПК РФ.

[3] Осипенко А.Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления // Вестник Воронежского института МВД России 2016. № 3. С. 83.

Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[1] дополнил этот перечень оперативно-розыскным мероприятием, названным «получение компьютерной информации». Появление ОРМ, учитывающего специфику доступа к информации в современных компьютерных системах, требует детального уяснения сущности и содержания нового мероприятия, проработки основ его практического осуществления.

До недавнего времени нормативное правовое закрепление близких по содержанию действий было предложено в модельном законе «Об оперативно-розыскной деятельности»,[2] где было названо соответствующее мероприятие, - «Мониторинг информационно-телекоммуникационных сетей и систем», которое определялось как «получение сведений, необходимых для решения конкретных задач оперативно-розыскной деятельности, и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам».

Полагаем, что данное определение не дает достаточно четкого представления о содержании рассматриваемого ОРМ. Кроме того, в общепринятом понимании термин «мониторинг» связывается со сбором, анализом и оценкой информации в определенной сфере, деятельностью по наблюдению за соответствующими явлениями, и его использование вряд ли можно признать удачным

---

[1] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Закон Российской Федерации от 06 июля 2016 г. № 374-ФЗ // Собрание законодательства РФ. 2016. № 28. Ст. 4558.

[2] Модельный закон «Об оперативно-розыскной деятельности (новая редакция)» (принят на XXVII пленарном заседании Межпарламентской Ассамблеи государств участников СНГ (постановление от 16 ноября 2006 года № 27-6) [Электр. ресурс] // СПС «КонсультантПлюс».

для обозначения действий, направленных на получение компьютерной информации.

Полагается, что в техническом плане получение компьютерной информации может осуществляться:[1]

а) при доступе (непосредственном или дистанционном через компьютерную сеть) к устройствам памяти, установленным в компьютере и периферийном оборудовании;

б) при копировании данных с внешних устройств хранения информации;

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

Во всех случаях информация может быть получена в виде отдельных текстовых, графических, аудио-и видео документов либо выборок по заданным условиям из специализированных баз данных.

С учетом изложенного, далее можно уяснить, каково содержание ОРМ «Получение компьютерной информации» с позиций оперативно-розыскной науки и практики.

Анализ положений Федерального закона об ОРД показывает, что законодатель вряд ли связывает его с простейшими формами обращения к компьютерным ресурсам, находящимся у операторов связи или в открытом доступе, либо к устройствам хранения компьютерной информации, полученным в распоряжение субъектов оперативно-розыскной деятельности. Такие действия, осуществляемые, как правило, гласно и не подразумевающие необходимости преодоления определенных препятствий, в большинстве случаев разумно оформлять через иные ОРМ (наведение справок, сбор образцов для сравнительного исследования, проводимое гласно обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.).

---

[1] Осипенко А.Л. Указ. соч. С. 85.

Основу ОРМ «получение компьютерной информации», очевидно, составляют достаточно сложные в техническом плане и требующие специальной подготовки действия по добыванию хранящейся в компьютерных системах или передаваемой по техническим каналам связи информации о лицах и событиях, вызывающих оперативный интерес. В большинстве случаев их правильное осуществление невозможно без участия специалиста. Об этом, в частности, свидетельствует и указание в части 4 ст. 6 ФЗ об ОРД на то, что ОРМ, связанные с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов Федеральной службы безопасности и органов внутренних дел.

Для определения конкретных действий, способных обеспечить получение компьютерной информации в рамках анализируемого ОРМ, целесообразно выделить потенциальные источники оперативно значимых компьютерных данных.

Эти источники могут быть разделены на четыре вида, в каждом из которых имеется своя специфика получения компьютерных данных.[1]

К техническим объектам такого рода могут быть отнесены:

а) потенциально содержащие сведения о разрабатываемых лицах средства вычислительной техники, включая средства сотовой связи и мобильные устройства, обеспечивающие доступ к сетевым ресурсам;

б) носители компьютерной информации, на которых могут храниться данные, представляющие оперативный интерес;

в) устройства, фиксирующие компьютерные данные, поступающие от различных датчиков (радиочастотных идентификаторов, GPS-трекеров, нательных датчиков, передающих физиологические показатели и сведения о местоположении, и т.п.), стационарных и мобильных измерительных устройств, систем геопозиционирования, видеонаблюдения и видеофиксации;

г) сетевое оборудование, через которое осуществляются коммуникационные акты разрабатываемых лиц.

---

[1] Осипенко А.Л. Указ. соч. С. 86.

Представляется, что спектр технических источников оперативно значимой информации в ближайшее время будет расширяться и за счет новых видов так называемых «умных вещей», оснащенных микропроцессорами и способных осуществлять обмен данными с телекоммуникационными сетями (навигационные системы автотранспорта, системы «умного дома», бытовые приборы, информационные датчики в местах общественного пользования и т.п.). Смена в современном обществе концепции «Интернет вещей» на «Интернет всего» предполагает подключение к сети практически всех объектов и инфраструктур, обслуживающих интересы как отдельных граждан, так и общества в целом. Понятно, что в потоках данных, формируемых в соответствующих системах, объективно присутствуют значительные объемы информации, представляющей интерес для оперативно-розыскных органов.

Получение оперативно значимой компьютерной информации предполагает обследование информационных объектов сети Интернет, среди которых можно выделить:

а) информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих (сайты криминальных структур, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту, ведется пропаганда криминального образа жизни, вовлекаются в противоправную деятельность новые участники и т.п.);

б) места сетевого общения (закрытые сетевые форумы и чаты (MAZAFAKA, Verified, Dark Money и т.д.), сообщества криминальной направленности в социальных сетях и др.) криминально настроенных лиц и их персональные страницы в социальных сетях.

Оперативно значимая информация на указанных объектах может концентрироваться в виде следов противоправной деятельности, ссылок на материалы, запрещенные к распространению, сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений.

Среди источников получения оперативно значимой компьютерной информации особое место занимают сетевые каналы коммуникации, задействованные преступниками для координации действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (Интернет-телефонии), мессенджеров и т.п. Обнаружение и контроль таких каналов оперативными подразделениями обеспечивает им существенные преимущества. При этом важно учитывать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через Интернет, постоянно увеличивается (ICQ, Skype, WhatsApp, Viber, Telegram и др.), причем многие из них предоставляют услуги шифрования передаваемых данных. Оперативно значимая информация может быть получена и из таких источников, как выборки, генерируемые по заданным условиям при анализе сведений из различных баз данных, формируемых в информационных системах государственных органов и коммерческих структур, в том числе банков и операторов связи.

С учетом изложенного можно определить, что содержание ОРМ «получение компьютерной информации» связано с применением особых способов доступа к перечисленным информационным источникам для достижения указанного в названии мероприятия результата. К таким способам, в частности, могут быть отнесены:

1. Негласное применение специального программного обеспечения и оборудования для съема данных с компьютерных устройств, потенциально содержащих оперативно значимую информацию, включая скрытый дистанционный доступ к компьютерам, имеющим сетевое подключение. Речь здесь, как правило, идет о доступе к информации, которую разрабатываемые лица размещают на закрытых сетевых ресурсах или хранят в своих компьютерных системах и, возможно, не намереваются куда-либо передавать.

2. Оперативно-розыскной мониторинг представляющих оперативный интерес сетевых информационных ресурсов, реализуемый через: автоматизиро-

ванный поиск ресурсов, содержащих запрещенную к распространению информацию; оперативно-розыскное изучение материалов выявленных ресурсов, связанных с деятельностью преступных сообществ; наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности.[1]

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

4. Применение аналитического программного обеспечения для выявления оперативно значимой информации в базах данных различного назначения. В простейших случаях соответствующие выборки могут представляться по запросу органа, осуществляющего оперативно-розыскную деятельность, в рамках ОРМ «Наведение справок». Однако есть ситуации, когда субъект ОРД заинтересован в получении от владельца базы данных непосредственного доступа к ней для обнаружения сложных неявных связей между объектами оперативного интереса путем анализа массивов неструктурированных данных из различных источников.

5. Проведение вербовочных мероприятий в отношении администраторов форумов, где злоумышленники обманом получают доступ к форумам, скрывая сведения об их действительных IP адресах.

6. Вербовка обменных сервисов Биткойн (Криптографическая валюта, а также электронная наличность), через которые преступники обналичивают денежные средства.

---

[1] Осипенко А.Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы // Научный вестник Омской академии МВД России. 2010. № 2. С. 38-43.

Криптовалюта – цифровые счетные единицы, учет которых децентрализован. Функционирование данных систем происходит при помощи распределенной компьютерной сети. При этом информация о транзакциях обычно не шифруется и доступна в открытом виде. Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование). Термин закрепился после публикации статьи о системе Биткойн «Crypto currency» (Криптографическая валюта), опубликованной в 2011 году в журнале Forbes. Для эмиссии криптовалют применяют различные способы: майнинг, форжинг или IPO.

ЗАКЛЮЧЕНИЕ

Подводя итоги, необходимо отметить, что деятельность оперативных подразделений, обеспечивающих раскрытие и своевременное реагирование на преступления в сфере высоких технологий с использованием вредоносных компьютерных программ, недостаточно проработана, но приобретает особую значимость в связи с компьютеризацией и глобальным использованием сети Интернет.

В целом, обобщенные выводы проведенного исследования можно представить следующим образом:

1. Исходя из статистических данных ГИАЦ МВД России за 2016 год, структура российской компьютерной преступности представлена широким спектром корыстных преступлений, совершаемых с использованием компьютерной информации. Существенную долю в нем занимают преступления, квалифицируемые по ст. 159.6 УК РФ.

2. Важное значение в организации ОРД по борьбе с мошенничеством, совершаемым с использованием компьютерной информации, имеет правильная уголовно-правовая квалификация содеянного. Уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю).

По нашему мнению, отсутствие прямо подтвержденных «ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» (либо «неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации») вызывает затруднение при квалификации преступления по ст. 159.6 УК РФ или возможно альтернативным ст. 272 и 273 УК РФ. В отдельных случаях следствием могут быть

усмотрены признаки кражи (ст. 158 УК РФ) или «простого» мошенничества (ст. 159 УК РФ).

Перспектива возбуждения дела с неопределенной квалификацией и возможной последующей переквалификацией, с отсутствующим или крайне затянувшимся экспертным исследованием, без выявленных лиц, без получателя денежных средств и с весьма слабой в целом перспективой раскрытия воспринимается сотрудниками полиции негативно. Поэтому зачастую на практике используются любая возможность и любые основания для отказа в возбуждении уголовного дела по поступившим заявлениям, что оставляет данные преступления безнаказанными.

3. Основную работу по выявлению, предупреждению, пресечению и раскрытию преступлений в сфере компьютерной информации выполняют оперативные подразделения органов внутренних дел, такие как Управление «К» БСТМ МВД России, отделы «К» БСТМ МВД, ГУМВД и УМВД субъектов РФ, специализированные отделы ГУЭБиПК МВД России и подразделений экономической безопасности МВД, ГУМВД и УМВД субъектов РФ, а также некоторые подразделения уголовного розыска. По нашему мнению, целесообразно проводить обучение, подготовку специалистов в сфере компьютерных преступлений для более эффективной работы подразделений уголовного розыска путем организации специализированных курсов для сотрудников, повышающих их навыки в технической части противодействия преступлениям в сфере высоких технологий.

4. На начальном этапе раскрытия преступлений в сфере телекоммуникаций и компьютерной информации немаловажное значение имеет своевременное получение информации о совершенном или готовящемся преступлении данной направленности. Полученная информация позволит оперативным сотрудникам избрать правильную линию поведения с целью определения необходимого осуществления первоначальных оперативно-розыскных, специальных технических мероприятий и следственных действий. Данное обстоятель-

ство поможет с наименьшей затратой времени выйти на более точное оперативно-розыскное обеспечение по установлению конкретных лиц, причастных к совершенному преступлению, и, как положительный результат, приведет к изобличению фигурантов с закреплением полученных в ходе документирования доказательств.

5. Целью уголовно-процессуального взаимодействия является получение относимых, допустимых, достаточных и достоверных доказательств, которые имеют не только процессуальную, но и тактическую природу. Вместе с тем принятие решения о проведении оперативно-технических мероприятий неминуемо влечет за собой определенные ограничения конституционных прав и свобод граждан, в связи с чем должны быть соблюдены все условия о недопустимости разглашения любых (полученных) данных, необходимых в дальнейшем, с их практической реализацией в процессе доказывания преступной деятельности разрабатываемых лиц, подозреваемых в совершении преступления.

6. В настоящее время методы и познавательные технологии, используемые сотрудниками оперативных подразделений, во многих случаях не позволяют сохранять процессуальную безупречность криминалистически значимой информации, полученной при производстве оперативно-розыскных мероприятий с использованием технических возможностей. Иными словами, при производстве оперативно-технического мероприятия не всегда удается добиться соблюдения всех требований, предъявляемых уголовно-процессуальным законом к доказательствам. В результате зачастую собранные оперативными сотрудниками сведения о задокументированных действиях лиц могут признаваться судом недопустимыми в доказывании их преступной деятельности в ходе судебного рассмотрения и окончательного разрешения по уголовным делам.

СПИСОК ЛИТЕРАТУРЫ

Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята 12 декабря 1993 г. – М.: Омега-Л, 2016.
2. Уголовный кодекс Российской Федерации о т 13 июня 1996 г. № 63 –ФЗ:с изм. и доп. - М.: Норматика, 2016.
3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: с изм. и доп. – М.: Проспект, 2016.
4. Об оперативно-розыскной деятельности: Федеральный закон РФ от 12 августа 1995 года № 144-ФЗ: с изм. и доп. – М.: Эксмо-Пресс, 2017.
5. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный Закон Российской Федерации от 06 июля 2016 г. № 374-ФЗ // Собрание законодательства РФ - 2016.- № 28. - Ст. 4558.
6. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента РФ от 9 мая 2017 г. № 203 // СПС «Консультант Плюс».
7. Модельный закон «Об оперативно-розыскной деятельности (новая редакция)» (принят на XXVII пленарном заседании Межпарламентской Ассамблеи государств участников СНГ (постановление от 16 ноября 2006 года № 27-6) [электронный ресурс] // СПС КонсультантПлюс.
8. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 // Бюллетень Верховного Суда РФ. 2008. № 2.

Монографии, учебники, учебные пособия

9. Акимова Т. А. Теория организации: учебное пособие для вузов / Т. А. Акимова. М., 2003.
10. Выявление и раскрытие мошенничества : учеб. пособие / под общ.ред. В.П. Сальникова. С-Пб; Лань, 2000.
11. Дуленко В.А. Преступление в сфере высоких технологий: учебное пособие / В.А. Дуленко Р.Р. Мамлеев, В.А. Пестриков. – М.: ЦОКР МВД России, 2010.
12. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий: учебно-практическое пособие. – М.: Академия управления МВД России, Следственный департамент МВД России, 2016.
13. Саввинов А. Г. Методика анализа и оценки управленческой деятельности: лекция / А. Г. Саввинов. – М., 1996.
14. Теория организации: учебник / Под общ. ред. Г. В. Атаманчука. М., 2007.
15. Токарев Е. В. Основы организации оперативно-розыскной деятельности органов внутренних дел и пути ее совершенствования: лекция / Е. В. Токарев. – М., 1994.

16. Туманов Г. А. Организация управления в сфере охраны общественного порядка / Г. А. Туманов. – М., 1972.

17. Яблоков Н. П. Криминалистика: учебник. Н.П. Яблоков – М.: ЛексЭст, 2006.

Статьи, научные публикации

18. Атмажитов В. М. Некоторые аспекты определения сущности организации оперативно-розыскной деятельности органов внутренних дел по борьбе с бандитизмом / В. М. Атмажитов, А. И. Музеев // Вестник Казанского ЮИ. – Казань: КЮИ МВД России, 2012. – № 1. С. 68-74.

19. Классификация криминалистически значимых признаков организованного мошенничества. / А.П. Ледяев // Российский судья. 2011, № 9. С. 25-30.

20. Кочкина С. В. Субъективная сторона мошенничества / Вестник Барнаульского юридического института МВД Рос. 2006 - № 10 - С. 16-21.

21. Сложности квалификации мошенничества / О.В. Михаль/ Уголовное право. 2009, № 6. С. 32-37.

22. Осипенко А. Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы / А. Л. Осипенко // Научный вестник Омской академии МВД России. 2010. №2. С. 38-43.

23. Осипенко А. Л. Новое оперативно-розыскное мероприятие «получение компьютерной информации»: содержание и основы осуществления / А. Л. Осипенко // Вестник Воронежского института МВД России – 2016-№3. С. 83-90.

24. Фролов М. Д. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации / М.Д. Фролов // Адвокат. 2016 - № 6 - С. 53-58.

25. Шмонин А. В. Методическое обеспечение организации выявления, раскрытия и расследования хищений денежных средств в системе дистанционного банковского обслуживания. / А. В. Шмонин // Расследование преступлений: проблемы и пути их решения. - М.: Московская академия Следственного комитета Российской Федерации. 2014 - №6 - С. 310-319.

Электронные ресурсы

26. Kaspersky security bulletin 2016: развитие угроз. URL: https://press.kaspersky.com/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016_итоги.pdf (дата обращения 10.04.2017).

27. Информационная безопасность (InformationSecurity): Интернет-ресурс http://www.itsec.ru/main.php

28. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Электронный ресурс. URL: http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb=1&pb=1.

29. Официальный отзыв от 2.08.2012 г. № 3904п-П4 на проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошен-

ничества на отдельные составы) // Справочная правовая система «Консультант Плюс».

30. Письмо Верховного Суда от 25 мая 2012 г. № 2-ВС-2733/12 // Справочная правовая система «Консультант Плюс».

31. Пояснительная записка к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации» (в части дифференциации мошенничества на отдельные составы) // Справочная правовая система «Консультант Плюс».

32. Богданов А. А. Очерки организационной науки. М., 1922. URL: http://www.uic.unn.ru/pustyn/lib/bogdanov.ru.html (дата обращения 10.04.2017).