РЕСПУБЛИКА КАЗАХСТАН
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
КАРАГАНДИНСКАЯ АКАДЕМИЯ им. БАРИМБЕКА БЕЙСЕНОВА
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
Центр по исследованию проблем следственной деятельности ОВД

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по досудебному расследованию уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют

Караганда, 2021

Составители: Центра по исследованию проблем следственной деятельности ОВД НИИ МВД РК им. Б. Бейсенова совместно со Следственным департаментом МВД Республики Казахстан

Методические рекомендации подготовлены в рамках научного исследования по теме «Совершенствование досудебного производства по уголовным делам», проводимого сотрудниками Центра по исследованию проблем следственной деятельности ОВД Научно-исследовательского института Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова

Содержание

I. ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ, А ТАКЖЕ СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПОТВАЛЮТ

Перечень уголовных правонарушений в сфере информатизации и связи составляют уголовные правонарушения, предусмотренные главой 7 УК:

1) неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205 УК);

2) Неправомерные уничтожение или модификация информации (ст. 206 УК);

3) Нарушение работы информационной системы или сетей телекоммуникаций (ст. 207 УК);

4) Неправомерное завладение информацией (ст. 208 УК);

5) Принуждение к передаче информации (ст. 209 УК);

6) Создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК);

7) Неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211 УК);

8) Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212 УК);

9) Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213 УК).

Предупреждение уголовных правонарушений в сфере информатизации и связи – деятельность по своевременному обнаружению и устранению либо нейтрализации (обезвреживанию, взятию под оперативный контроль) криминальных угроз[1] информационной безопасности[2].

1.1. Угрозы информационной безопасности

Основные виды криминальных угроз информационной безопасности:

1. Угроза нарушения конфиденциальности – риск возникновения ситуации, когда информация становится известной тому, кто не располагает полномочиями доступа к ней. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место, когда получен доступ к некоторой информации закрытого (конфиденциального) характера, хранящейся в вычислительной системе или передаваемой от одной системы к другой.

[1] Криминальная угроза – объективная опасность совершения уголовно наказуемого посягательства (уголовного правонарушения), имеющая определенную степень вероятности, а также объективная опасность возникновения массовой тенденции совершения уголовных правонарушений определенного вида.

[2] Информационная безопасность – родовой объект уголовных правонарушений в сфере информатизации и связи, который характеризует состояние защищенности охраняемой законом информации и объектов информатизации, в том числе систем и оборудования, предназначенные для обработки, использования, сбережения и передачи охраняемой законом информации.

2. Угроза нарушения целостности – риск возникновения ситуации, когда совершается любое умышленное неправомерное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда правонарушитель преднамеренно изменяет охраняемую законом информацию, нарушает ее целостность.

3. Угроза отказа служб возникает, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Основные направления (методы) реализации криминальных угроз информационной безопасности:

– непосредственный незаконный доступ к охраняемой законом информации и (или) информационным системам;

– создание программных и технических средств, выполняющих обращение к автоматизированным системам в обход средств защиты;

– модификация средств защиты с целью незаконного доступа к защищенной информационной системе;

– внедрение в технические средства защищенной информационной системы программных или технических механизмов, нарушающих ее нормальную деятельность (например, внедрение компьютерных вирусов).

К числу основных методов реализации угроз информационной безопасности информационных систем относятся:

– определение злоумышленником типа и параметров носителей информации;

– получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;

– получение злоумышленником детальной информации о функциях, выполняемых информационной системой;

– получение злоумышленником данных о применяемых системах защиты;

– определение способа представления информации;

– определение злоумышленником содержания данных, обрабатываемых в АС, на качественном уровне (применяется для мониторинга информационной системы и для дешифрования сообщений);

– хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;

– использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН) – конфиденциальные данные перехватываются злоумышленником путем выделения информативных сигналов из электромагнитного излучения и наводок по цепям питания средств вычислительной техники, входящей в информационную систему;

– уничтожение средств вычислительной техники и носителей информации;

– хищение (копирование) носителей информации;

– несанкционированный доступ пользователя к ресурсам информационной системы в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;

– несанкционированное превышение пользователем своих полномочий;

– несанкционированное копирование программного обеспечения;

– перехват данных, передаваемых по каналам связи;

– визуальное наблюдение – конфиденциальные данные считываются с экранов терминалов, распечаток в процессе их печати и т.п.;

– раскрытие представления информации (дешифрование данных);

– уничтожение машинных носителей информации;

– внесение пользователем несанкционированных изменений в программно-аппаратные компоненты информационной системы и обрабатываемые данные;

– установка и использование нештатного аппаратного и(или) программного обеспечения;

– заражение программными вирусами;

– внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;

– внедрение дезинформации;

– выведение из строя машинных носителей информации без уничтожения информации – выведение из строя электронных блоков накопителей на жестких дисках и т.п.;

– проявление ошибок проектирования и разработки аппаратных и программных компонентов информационной системы;

– обход (отключение) механизмов защиты – загрузка злоумышленником нештатной операционной системы с дискеты, использование отладочных режимов программно-аппаратных компонент информационной системы и т.п.;

– искажение соответствия синтаксических и семантических конструкций языка – установление новых значений слов, выражений и т.п.;

– запрет на использование информации – имеющаяся информация по каким-либо причинам не может быть использована.

1.2. Предупреждение уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют

Меры предупреждения уголовных правонарушений в сфере информатизации, а также совершаемых с использованием криптовалют, направлены непосредственно на устранение их причин и условий.

Основные мерами предупреждения уголовных правонарушений данного вида заключаются в обеспечении высокого уровня государственного контроля над субъектами и каналами оборота цифровой информации в сети Интернет и оборотом криптовалют. Однако по объективным причинам проблема обеспечения такого контроля остается нерешенной (у государственных органов Республики Казахстан не имеется достаточных административных ресурсов для воздействия на основных

операторов информационного обмена в сети Интернет, которые осуществляют свою деятельность в иностранных юрисдикциях – Google, Facebook, Telegram, Яндекс и др.). В Республике Казахстан отсутствует правовой режим эмиссии и оборота криптовалют.

В целом, как для Республики Казахстан, так и для большинства других стран, фундаментальной проблемой является отсутствие сформировавшегося международного информационного права, которым бы регулировались все общественные отношения, возникающие в связи с созданием, размещением, обменом, использованием, хранением и уничтожением цифровой информации и информационно-цифровых продуктов, а также отсутствие единого международного органа (центра) управления и контроля над глобальным информационно-цифровым оборотом.

В этой связи, перечень и потенциал мер профилактики уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют, является достаточно узким.

Специалистами в области информационной безопасности для создания эффективной системы контроля над цифровым интернет-пространством предлагается создание единой международной базы данных электронно-цифровых следов в криминалистических целях. С помощью современных технологий цифрового анализа (Big Data, Machine Learning и др.) станет возможным идентифицировать (по множеству параметров) каждое техническое устройство, с помощью которого осуществляется посягательство. Такой подход позволит определить конкретный смартфон, компьютер или планшет с высокой точностью. Совпадение электронно-цифрового следа, выявленного при совершении преступления, будет фактически равно установлению личности пользователя (правонарушителя).

Особенность уголовных правонарушений в сфере информатизации (потребность в специалистах, обладающих специальными познаниями в области компьютерной техники, технологий и навыками обращения с цифровой информацией), требуют привлечения к профилактическим мероприятиям специалистов в сфере информационных технологий.

Следует выделить следующие направления и наиболее важные аспекты профилактики уголовных правонарушений в сфере информатизации.

1. Использование ресурсов Интерпола для быстрого и эффективного обмена оперативно значимой информацией об уголовных правонарушениях в сфере информатизации и связи, уголовных правонарушений, совершаемых с использованием криптовалют, и лицах, вовлеченных в данную криминальную деятельность (прежде всего в отношении транснациональных киберпреступлений).

2. Совершенствование информационно-аналитической деятельности ОВД по противодействию уголовным правонарушениям, совершаемым в сфере информатизации.

Формирование ведомственной базы данных оперативно-значимой информации и информационно-аналитической базы специальных оперативных

учетов о лицах, организациях, связанных с киберпреступностью, а также специальных оперативных учетов.

3. Усиление мер цифровой безопасности информационных систем в государственном и частном секторах *(организация профилактических агитационных мероприятий в СМИ, проведение профилактических разъяснительных мероприятий с собственниками и управляющими коммерческих и некоммерческих организаций*.

4. Усиление взаимодействия ОВД со средствами массовой информации.

Использование средств массовой информации в системе противодействия высокотехнологичной преступности должно сочетать несколько направлений, таких как отчет перед населением о результатах борьбы с данными преступлениями; проведение правовой пропаганды, направленной на формирование правосознания и нетерпимости к преступным проявлениям; информирование населения о средствах и методах защиты от мошеннических посягательств, о новых формах его осуществления.

К работе со СМИ необходимо привлекать и общественные организации, заинтересованные в противодействии киберпреступности, а также IT-компании, специализирующиеся на информационной безопасности.

5. Усиление защитных мер в регулировании трудовых отношений в организациях, осуществляющих деятельность в сфере информатизации: при заключении индивидуальных трудовых договоров с работниками, получающими доступ к защищаемой законом информации, предусмотреть расписку о неразглашении и недопущении доступа к такой информации, а также предупреждение персональной ответственности таких работников за разглашение, утрату защищаемой законом информации, а также за неправомерный доступ к информации и (или) информационным системам третьим лицам.

6. Отдельным направлением профилактики преступлений в сфере информатизации является виктимологическая профилактика (т.е. профилактическая работа с потенциальными жертвами по недопущению и устранению допущенных факторов, провоцирующих потенциальных правонарушителей на посягательство).

Основной формой виктимологической профилактики является распространение через СМИ профилактических видеоматериалов, наглядных памяток о наиболее распространенных ситуациях, видах и способах противоправных посягательств в сфере информатизации и связи.

Рекомендуется обращать внимание на три основных фактора, позволяющих изобличить (выявить) попытку совершения уголовного правонарушения в сети Интернет:

1) визуальная оценка.

Рекомендации интернет-пользователям могут состоять в следующем:

«необходимо особое внимание уделять внешнему оформлению (дизайну) интернет-ресурса, запрашивающего персональные данные (например, интернет-магазина) (не нужно принимать в качестве достоверных отзывы пользователей, размещенные на этом же сайте, которые, как правило, имеют свежую дату и содержат избыточную, неестественную похвалу; необходимо искать отзывы о

данном интернет-ресурсе на других сайтах; необходимо обращать внимание на то, какую площадь веб-страницы занимает баннерная реклама; положительную оценку получают сайты, не имеющие ни одной рекламной площадки или имеющие рекламу своих дочерних или, наоборот, головных предприятий; присутствие рекламы означает, что магазин зарабатывает прибыль не на продаже товаров)».

Целесообразно рекомендовать интернет-пользователям применять наиболее подходящий, защищенный и правильно настроенный веб-браузер, который незамедлительно предупреждает о возможной опасности. Это касается не только браузеров, но и других используемых программ (например, электронных кошельков WebMoney).

2. Ценовая политика.

Рекомендации интернет-пользователям могут состоять в следующем:

«необходимо понимать, что цена товара определяется рынком и не может резко отличаться от средней; в Интернете достаточно сервисов, предоставляющих возможность поиска того или иного товара с определением средней стоимости товара среди множества предложений».

3. Условия и права.

Рекомендации интернет-пользователям могут состоять в следующем:

«особое внимание следует обратить на разделы сайта о самой организации и оказываемых услугах (сайты легальных организаций всегда размещают полную информацию о себе, осуществляемой деятельности и услугах, полную информацию о юридическом адресе и контактные данные; запрос сайта на регистрацию аккаунта и ввод персональных данных, зачастую, свидетельствует о противоправных целях владельца сайта).

Основные запреты (меры предосторожности), которые целесообрпазно рекомендовать населению при использовании Интернета:

– загрузки из сети Интернет программных продуктов из непроверенных источников; перехода по рекламным ссылкам в Интернете, сулящим бесплатные услуги, различные призы или существенные скидки; просмотра корреспонденции от неизвестных адресатов;

– общения в социальных сетях с незнакомыми пользователями, за которыми могут скрываться мошенники, сектанты, вербовщики в террористические организации;

– покупки SIM-карт с рук или оставления своих паспортных данных сомнительным конторам;

– отправки денежных переводов лицам, предлагающим посреднические услуги в разрешении проблем с родственниками, знакомыми, якобы попавшими в беду;

– передачи данных с кредитных или дебетовых карт, пользовательских паролей и кодовых слов, запрашиваемых по телефону или через социальные сети от лица друзей, знакомых, кредитных или иных организаций под различными предлогами;

– указания в своем профиле социальной сети личной информации, в том числе о своем образе жизни, планируемых отъездах и т. п.;

– проведения операций в интернет-банкинге без проверки истинности адреса личного кабинета или при наличии дополнительных не предусмотренных стандартной процедурой запросов (защита от «фишинга»);

– непринятия срочных мер по блокированию кредитных или дебетовых карт при получении SMS о несанкционированном списании или переводе средств третьим лицам;

– регистрации в личных кабинетах, на интернет-ресурсах или онлайн-магазинах с простыми паролями, состоящими из нескольких цифр, коротких слов, соседних клавиш на клавиатуре, личных памятных дат, адресов или номеров телефонов;

– записей личных паролей на стикерах, приклеенных к монитору, или в других легкодоступных местах.

В рамках профилактических мероприятий не следует доводить до широких масс населения конкретные криминальные схемы, используемые правонарушителями, поскольку вариативность данных схем очень высокая, они регулярно обновляются. Транснациональный характер киберпреступности способствует возникновению «очаговых» схем, имеющих ограниченное распространение (локализованное в масштабах определенного государства или региона). Поэтому простое информирование населения о новых способах совершения мошенничества может иметь противоположный эффект: наиболее виктимные слои населения (пожилые люди, доверчивые и легкомысленные пользователи и т.д.) подобной информацией, скорее всего, не заинтересуются, а потенциальные правонарушители могут начать использовать данные криминальные схемы.

Таким образом, виктимологическая профилактика преступлений, совершаемых с использованием высоких технологий, должна:

– быть организована с учетом виктимности различных групп населения; учитывать различные аспекты обеспечения данного вида деятельности;

– иметь конкретную направленность на осознание необходимости соблюдения мер предосторожности в информационно-телекоммуникационном пространстве;

– основываться на доступных для населения или работников – неспециалистов рекомендациях по совершенствованию своей защищенности от киберугроз.

II. ОСОБЕННОСТИ РАСКРЫТИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ, А ТАКЖЕ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

2.1. Общие подходы к раскрытию уголовных правонарушений в сфере информатизации и связи, а также уголовных правонарушений, совершаемых с использованием криптовалют

При совершении уголовных правонарушений в сфере информатизации и связи (киберпреступлений) применяются средства, позволяющие скрыть реальную

личность кибер-правонарушителя (VPN/VPS-сервисы для анонимизации интернет-трафика, виртуальные номера мобильных телефонов и адреса электронной почты, анонимные электронные и криптовалютные кошельки). Персональные данные пользователя (ФИО) заменяется на никнейм (цифровой псевдоним), количество которых у злоумышленников может достигать нескольких десятков, дата рождения указывается вымышленная. При этом локация (место нахождения компьютера или иного технического устройства, при помощи которого совершается киберпреступления) также маскируются, в том числе посредством подложных IP-адресов.

Указанные обстоятельства существенно осложняют раскрытие уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют.

Раскрытие данных уголовных правонарушений после регистрации сведений в ЕРДР осуществляется процессуальным путем (в рамках досудебного расследования) посредством производства негласных следственных действий (далее – НСД).

Порядок проведения НСД регламентирован главой 30 Уголовно-процессуального кодекса Республики Казахстан.

При раскрытии и расследовании уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют, как правило, осуществляются следующие НСД (ст. 231 УПК):

1) негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации;

2) негласные контроль, перехват и снятие информации, передающейся по сетям электрической (телекоммуникационной) связи;

3) негласное получение информации о соединениях между абонентами и (или) абонентскими устройствами.

В соответствии со статьей 232 УПК, перечисленные НСД производятся по поручению органа досудебного расследования уполномоченным (оперативным) подразделением правоохранительного органа (ОВД) с использованием форм и методов оперативно-розыскной деятельности.

Лицо, вынесшее поручение, несет ответственность за его законность и обоснованность в соответствии с законом Республики Казахстан.

Порядок получения и исполнения поручения по НСД, а также порядок представления результатов НСД, их исследование и оценка закреплены в нормах Правил проведения негласных следственных действий (*утверждены совместным приказом Министра внутренних дел Республики Казахстан от 12 декабря 2014 года № 892, Министра финансов Республики Казахстан от 12 декабря 2014 года № 565, Председателя Агентства Республики Казахстан по делам государственной службы и противодействию коррупции от 12 декабря 2014 года № 62, Начальника Службы государственной охраны Республики Казахстан от 15 декабря 2014 года № 146 и Председателя Комитета национальной безопасности Республики Казахстан от 18 декабря 2014 года № 416 Министра внутренних дел РК от 12 декабря 2014 года № 892)»*.

2.2. Характеристика и содержание НСД, производимых в рамках раскрытия, расследования уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют

1. При производстве НСД «негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации (ст. 245 УПК РК)» осуществляется:

– сбор информации о месте, времени, техническом устройстве, условном имени пользователя, посредством которого был осуществлен вход информационную систему и совершено соответствующее киберправонарушение;

– сбор и анализ всех доступных цифровых следов и цифровой информации о характере деятельности фигуранта, зарегистрированного под соответствующими персональными данными (цифровым псевдонимом (никнеймом), IP-адресом).

2. При производстве НСД «негласные контроль, перехват и снятие информации, передающейся по сетям электрической (телекоммуникационной) связи» осуществляется:

– установление места и времени совершения уголовного правонарушения, орудия и средства совершения уголовного правонарушения (тип, вид технического устройства, посредством которого было совершено деяние) а также других цифровых данных, позволяющих установить цифровые и реальные (пространственные) координаты виновного (доменное имя, IP-адрес, MAC-адрес и др.);

– направить запросы интернет-провайдерам о предоставлении значимой для следствия информации, в том числе сведений о пользователе сети (фигуранте с соответствующим IP-адресом), сайтах и других интернет-ресурсах, которые он посещал, а также других действиях пользователя (фигуранта) за определенный период;

– получить и исследовать данные о транзакциях по лицевым счетам электронных кошельков (если деяние совершено по поводу криптовалюты или с ее использованием);

– если на оптических дисках и в распечатках с транзакциями по лицевым счетам электронных кошельков содержится информация о снятии денег путем использования банкоматов, то в соответствующие кредитные организации направляются запросы о владельцах банковских карт, местонахождении банкоматов, в которых были сняты деньги, предоставлении сведений с видеокамер слежения банкоматов о выполнении банковских операций по счетам указанной карты и т.п.

3. При производстве НСД «негласное получение информации о соединениях между абонентами и (или) абонентскими устройствами» осуществляется (производится в случае, если деяние совершено на территории Республики Казахстан, установлена личность фигуранта и идентификационные данные используемого им средства сотовой связи):

– осуществляется детализация и анализ входящих и исходящих переговоров, SMS-сообщений;

– устанавливается круг лиц, причастных к совершенному уголовному правонарушению.

III. ОСОБЕННОСТИ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ, А ТАКЖЕ СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

3.1 Типичные следственные ситуации и обстоятельства, подлежащие установлению при расследовании уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют

Типичные следственные ситуации.

Чаще всего поводами для начала досудебного расследования по фактам уголовных правонарушений в сфере информатизации и связи являются заявления заявления официальных представителей организаций (юридических лиц) и частных физических лиц (граждан).

Типичные следственные ситуации определяются по объему информации о преступнике с точки зрения благоприятности ее для расследования. Их можно классифицировать следующим образом:

1) деяние совершено посредством неправомерного вторжения в информационную систему (т.е. виртуальным способом), преступник не установлен.

Для таких ситуаций характерно производство таких следственных действий: осмотр компьютерной техники (с изъятием для производства экспертиз); назначение экспертиз в отношении изъятой компьютерной техники; допрос потерпевшего; допрос специалиста (с участием которого осуществлялся осмотр компьютерной техники); негласные следственные действия;

2) в ходе неотложных следственных и негласных следственных действий лицо, совершившее деяние, установлено, но не задержано.

В таких случаях проводятся: негласные следственные действия по установлению местонахождения лица и подтверждению его причастности к совершенному деянию; допросы свидетелей и других осведомленных лиц.

Очередность проведения указанных действий может меняться в зависимости от конкретных ситуаций. Кроме того, на первоначальном этапе могут проводиться и иные следственные действия;

3) в ходе неотложных следственных и негласных следственных действий лицо, совершившее деяние, установлено и задержано.

В этой ситуации производится допрос задержанного (доставленного) лица в качестве подозреваемого (или свидетеля, имеющего право на защиту); допросы новых свидетелей (в случае, если таковые будут установлены по результатам допроса задержанного лица); выемка и осмотр компьютерной и иной техники, находившейся в пользовании задержанного лица; обыск по месту жительства задержанного лица; назначение экспертиз в отношении техники, изъятой при выемке и обыске; негласные следственные действия (при необходимости).

Обстоятельства, подлежащие установлению:

– место, время и способ уголовно наказуемых действий в сети Интернет (в информационной системе);

– кто конкретно осуществлял уголовно наказуемых действий в сети Интернет (в информационной системе);

– в чем именно выражался противоправный характер действий лица, совершенных в сети Интернет (в информационной системе);

– вид и размер причиненного ущерба (вреда);

– средства и орудия совершения уголовного правонарушения в сети Интернет (в информационной системе), их местонахождение – конкретный компьютер, смартфон, планшет или иное техническое устройство, посредством или при помощи которого совершены уголовно-наказуемые действия в сети Интернет (в информационной системе);

– умысел лица на совершение уголовно-наказуемых действий, совершенных в сети Интернет (в информационной системе);

– мотив и цель совершения лицом уголовно наказуемых действий в сети Интернет (в информационной системе) (мотив и цель устанавливаются даже в том случае, если они не являются обязательными признаками субъективной стороны состава уголовного правонарушения; их установление необходимо для подкрепления доказательственной базы);

– если уголовное правонарушение совершено в группе, то личность и местонахождение соучастников и роль каждого из них в совершении уголовного правонарушения;

– каковы причины и условия, способствовавшие совершению уголовного правонарушения.

Перечень указанных обстоятельств не является окончательным в зависимости от конкретных обстоятельств дела он может быть дополнен.

3.2. Особенности регистрации в ЕРДР, первоначального и последующего этапов расследования уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют.

Как правило регистрация уголовных правонарушений в сфере информатизации и связи регистрируются по заявлению потерпевшего (частного физического лица или представителя юридического лица).

В подавляющем большинстве случаев уголовное правонарушение, совершенное в виртуальном пространстве, не имеет выраженных следов, информации о месте, времени, способе совершения и лице его совершившем. В таких случаях после регистрации в ЕРДР уполномоченное лицо направляет поручение о производстве негласных следственных действий (*о негласном снятии информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации; о негласном контроле, перехвате и снятии информации, передающейся по сетям электрической (телекоммуникационной) связи; о негласном получении информации о соединениях между абонентами и (или) абонентскими устройствами*).

Руководитель подразделения–исполнителя, получив поручение о производстве НСД, немедленно принимает меры по его выполнению и поручает проведение НСД сотруднику уполномоченного подразделения, который оформляет дело негласных следственных действий.

Орган досудебного расследования вправе в любое время истребовать от уполномоченного подразделения результаты проводимого ими мероприятия для исследования, оценки и приобщения к материалам расследования.

При проведении НСД оперативные сотрудники должны действовать в тесном взаимодействии со следователем или дознавателем, т.к. упущения или нарушения норм УПК могут повлечь за собой утрату или признание полученных данных недопустимыми в качестве доказательств.

После проведения первоначальных следственных действий и оперативно-розыскных мероприятий, если они завершились задержанием подозреваемого, на последующем этапе расследования проводятся: следственный эксперимент, очные ставки, допросы свидетелей, предъявления для опознания, допрос подозреваемого.

Своевременность проведенных следственных действий и экспертиз, позволит получить полную картину преступного события и позволит в дальнейшем обеспечить должную квалификацию совершенного уголовного правонарушения.

3.3. Особенности производства следственных действий при расследовании уголовных правонарушений в сфере информатизации и связи, а также совершаемых с использованием криптовалют

При расследовании дел данной категории, как правило, производятся следующие следственные действия:

– осмотр;

– допросы;

– выемка;

– обыск;

– назначение и производство судебных экспертиз *(судебно-экспертное исследование средств компьютерной технологии)*.

Осмотр места происшествия. Осмотр места происшествия производится, как правило, в случае, если по обстоятельствам дела точно или предположительно известно физическое место совершения уголовного правонарушения (т.е. место нахождения лица, совершившего уголовное правонарушении в момент его совершения) – квартира, служебное или производственное помещение и др.

Однако, поскольку по данной категории дел точное или предположительное физическое место совершения уголовного правонарушения не устанавливается, осмотр места происшествия при досудебном расследовании таких уголовных правонарушений, как правило, не производится. Осуществляется осмотр и выемка соответствующей компьютерной и иной техники, посредством которой потерпевшим установлен факт совершенного уголовного правонарушения.

Детальное исследование изъятой компьютерной и иной техники, включая цифровую информацию на электронных носителях и в сети Интернет, осуществляется в рамках производства соответствующих

Осмотр предметов (компьютерной, иной техники, электронных носителей информации).

Осмотр компьютерной техники и электронных носителей информации производится с обязательным участием специалиста.

Задачами специалиста при осмотре и изъятии компьютерной техники и электронных носителей информации являются:

– оказание консультативной помощи при выработке тактики проведения следственного действия;

– обнаружение средств экстренного уничтожения информации;

– определение способов нейтрализации средств экстренного уничтожения информации;

– выявление признаков применения «облачных» технологий хранения данных;

– обнаружение средств шифрования данных и криптографических контейнеров, фиксация их содержания;

– обнаружение систем дублирования и резервного хранения информации;

– оказание помощи следователю при составлении протокола в описании объектов;

– копирование данных, поиск и извлечение конкретной значимой информации;

– фиксация информации с удаленных сетевых ресурсов, выявление идентификационных данных;

– определение криминалистически значимых сведений об используемой операционной системе и программном обеспечении;

– обнаружение сведений о подключенных ранее к компьютеру электронных носителях.

При осмотре компьютерной техники (стационарный компьютер, ноутбук, планшетный компьютер, смартфон), с использованием которой потерпевший установил факт совершенного уголовного правонарушения, фиксируются:

– наличие на устройстве программного обеспечения, позволившего (обеспечившего техническую возможность) совершения противоправного деяния (например, незаконного вторжения и повреждения или завладения информационными ресурсами потерпевшего);

– иные цифровые следы (сообщения, запросы, переписка) действий виновного.

Осмотр электронного носителя информации осуществляется путем функционального исследования электронной информации, содержащейся на электронном носителе. При необходимости, в интересах следствия или в случае возврата электронного носителя информации законному владельцу, содержимое электронного носителя информации может быть скопировано в установленном порядке.

По результатам осмотра (в порядке выемки) устройство подлежит изъятию для последующего назначения и производства судебной экспертизы средств компьютерных технологий.

Обыск и выемка. Если в ходе расследования установлено (достоверно известно), что на месте происшествия или в другом месте имеются не изъятые

документы, предметы, имеющие значение для дела, необходимо произвести их выемку.

Выемке подлежит:

– компьютерная техника (со всеми обнаруженными комплектующими частями);

– вспомогательная и интегрированная техника хранения, обработки и обмена электронной информацией (серверы, рабочие станции и др.);

– связанная с компьютерной техникой оргтехника (копиры, сканеры и др.);

– иные электронные носители информации (карты памяти, флеш-накопители, съемные жесткие диски, компакт-диски и др.);

– иная техника и предметы, могущие иметь значение для дела.

Устанавливается особая (специальная) процедура изъятия электронных носителей информации в ходе производства осмотра, обыска или выемки, содержащая следующие требования:

– обязательное участие специалиста;

– обязательное копирование информации с изымаемых электронных носителей при одновременном наличии следующих условий: соответствующее ходатайство законного владельца изъятых электронных носителей или обладателя содержащейся на них информации;

– выполнение копирования специалистом, участвующим в осмотре, (обыске, выемке);

– предназначенные для копирования другие электронные носители предоставляются законным владельцем изъятых носителей или обладателем содержащейся на них информации;

– копирование информации не может воспрепятствовать расследованию преступления или повлечь за собой утрату или изменение информации;

– об осуществлении копирования информации и о передаче электронных носителей, содержащих скопированную информацию, законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации делается запись в протоколе осмотра (обыска, выемки).

Условиями правомерности копирования в ходе обыска или выемки информации, находящейся на электронных носителях, являются:

– поступление соответствующего ходатайства законного владельца изъятых электронных носителей или обладателя содержащейся на них информации;

– предоставление предназначенных для копирования электронных носителей законным владельцем изъятых носителей или обладателем содержащейся на них информации;

– разрешение поступившего ходатайства о производстве копирования информации с изымаемых носителей осуществляется следователем (дознавателем);

– выполнение копирования производится специалистом, участвующим в обыске (выемке);

– копирование не сможет воспрепятствовать расследованию преступления или повлечь за собой утрату или изменение информации (в 50 % изученных уголовных

дел в копировании информации отказывалось в связи с наличием вероятности воспрепятствования расследованию).

Упаковка изымаемых электронных носителей информации должна отвечать следующим требованиям:

– исключение возможности непроцессуальной работы с электронными носителями;

– недопущение физического повреждения, разукомплектования носителя, повреждения находящейся на нем информации (опечатывание клапанов упаковки производится таким образом, чтобы вскрытие было невозможно без повреждения опечатывающих наклеек;

При упаковке сам электронный носитель целесообразно помещать в специальную экранирующую тару («мешок Фарадея»).

Если в ходе выемки получить свободный доступ к предметам, документам, подлежащим изъятию, не представляется возможным (в их выдаче отказывает ответственное лицо, находятся в закрытом помещении и т.д.), производится принудительная выемка (п. 10 ст. 254 УПК) или обыск.

Если после производства выемки у следствия имеются достаточные основания полагать, что часть предметов, документов, имеющих значение для дела, не изъяты из-за сокрытия их заинтересованными лицами (лицом, совершившим деяние, его родственниками или близкими), после выемки целесообразно произвести обыск.

Особенности признания электронных носителей информации вещественными доказательствами.

Электронные носители информации признаются вещественными доказательствами и приобщаются к уголовному делу в случаях, если они:

– служили орудиями, оборудованием или иными средствами совершения преступления;

– сохранили на себе следы преступления;

– являлись предметом преступного посягательства;

– могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

О признании электронных носителей информации вещественными доказательствами выносится соответствующее постановление.

Устанавливаются специальные требования к хранению электронных носителей:

– в опечатанном виде;

– в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией;

– в условиях, обеспечивающих сохранность как самих электронных носителей, так и содержащейся на них информации.

Электронный документ, содержащийся на электронном носителе, является иным документом, если он отвечает требованиям относимости и допустимости, заверен электронной подписью, обладает реквизитами и не содержит признаков вещественного доказательства (ответы на запросы, справки, официальная переписка и пр.).

Электронные носители информации, не признанные вещественными доказательствами, подлежат возврату лицам, у которых они были изъяты.

Назначение судебных экспертиз. Назначается судебно-экспертное исследование средств компьютерной технологи в отношении изъятой компьютерной и иной техники, а также электронных носителей информации.

Объектами экспертного исследования, как правило, являются:

1) Аппаратные объекты:

– различные виды персональных компьютеров (настольные, портативные, карманные и так далее) с основными блоками (системные блоки, мониторы), внутренними узлами, деталями, комплектующими и так далее (далее – ЭВМ);

– периферийные устройства различного вида и назначения;

– сетевые аппаратные средства (северы, рабочие станции, активное оборудование, сетевые кабели и т.д.);

– дисковые накопители данных (жесткие диски HDD, флоппи-диски FDD, оптические компакт-диски CD-ROM, CD-RW, DWD-ROM, флэш-карты USB).

2) Программные объекты:

– системное программное обеспечение (различные операционные системы для персональных компьютеров и локальных сетей MS-DOS, UNIX, Windows различных версий и так далее, вспомогательные программы – утилиты, средства разработки и отладки программ, служебная системная информация и так далее);

– различные прикладные программные продукты (приложения общего назначения: текстовые и графические редакторы, системы управления базами данных, электронные таблицы, редакторы презентаций;

– приложения специального назначения для решения задач в определенной области науки, техники, экономики и так далее).

3) Информационные объекты:

– файлы, подготовленные с использованием указанных выше и других программных средств (с расширениями текстовых форматов .txt, .doc, графических форматов .bmp, .jpg, .cdr, форматов баз данных .dbf, .mdb, электронных таблиц .xls, .cal и др.).

– данные в форматах мультимедиа.

4) Объекты, содержащие информацию, необходимую для производства экспертных исследований:

– различные документы (договоры на покупку, создание (передачу) научно-технической продукции;

– акты сдачи-приема научно-технической продукции;

– калькуляции стоимости предпродажной подготовки компьютерной техники и периферийных устройств и прочие);

– сопроводительная документация к поставляемой на исследование компьютерной, вычислительной технике (периферийным устройствам, магнитным носителям), различные справочные данные, инструкции пользователя, а также материалы дел.

Задачи, решаемые в рамках данной методики, относятся к задачам диагностического, классификационного, идентификационного и ситуационного характера.

При производстве данной экспертизы решаются следующие вопросы:

1) По аппаратным средствам:

– каковы технические характеристики представленной компьютерной техники;

– возможно ли использование представленного технического комплекса для осуществления тех или иных функциональных задач (например, выхода в Интернет, запись компакт-дисков);

– каковы ориентировочные даты создания вычислительного комплекса с заданными возможностями и даты изготовления его отдельных блоков.

2) По программным продуктам:

– какая операционная система установлена в представленном системном блоке;

– имеется ли в представленном системном блоке установленное программное обеспечение (указывается название);

– находится ли данное программное обеспечение в работоспособном состоянии;

– каковы дата и время установки программного обеспечения (указывается название);

– имеются ли в предоставленных системных блоках программы, приводящие к неправомерному доступу к охраняемой законом компьютерной информации, внесению изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ;

– каковы основные функции представленного программного обеспечения;

– каково назначение представленных программ для ЭВМ;

– возможно ли осуществление заданного вида деятельности с использованием представленных технических средств и размещенного на нем информационного и специального программного обеспечения (запись компакт-дисков, подготовка и изготовление поддельных денежных знаков).

– 3) По информационным объектам:

– имеется ли на представленном магнитном диске или в составе технических средств вычислительной техники необходимое информационное обеспечение для решения какой-либо конкретной функциональной задачи;

– имеются ли на представленных магнитных носителях файлы с документами, относящимися к той или иной сфере деятельности (файлы с изображениями денежных знаков, бланками юридических лиц и оттисками печатей);

– имеются ли на представленных магнитных носителях ранее удаленные файлы (указываются названия);

– имеются ли на магнитном носителе какая-либо информация, если да, то каков вид ее представления;

– каково дата и время создания файлов (указываются названия).

Допрос.

По процессуальному положению допрашиваемого допросы подразделяется на:

– допрос свидетеля;

– допрос эксперта (специалиста);

– допрос подозреваемого, свидетеля, имеющего право на защиту;

– допрос потерпевшего.

По делам данной категории, особое внимание необходимо уделить допросу потерпевшего, специалиста (эксперта), и подозреваемого.

Как правило, на первоначальном этапе досудебного расследования производится допрос потерпевшего (т.к., зачастую, это единственное лицо, владеющее информацией об уголовном правонарушении, совершенном в виртуальном пространстве).

При **допросе потерпевшего** следует выяснить:

– обстоятельства совершенного уголовного правонарушения и его обнаружения (в чем именно оно выразилось деяние и его криминальные последствия);

– предметы компьютерной техники, иных технических устройств, посредством которых обнаружено уголовное правонарушение, а также регулярно используемые потерпевшим для выхода в сеть Интернет и использования информационных систем,

– характер и размер причиненного вреда (ущерба);

– вероятный круг подозреваемых лиц.

При **допросе свидетеля** следует выяснить:

– сведения о деятельности потерпевшего, связанной с обстоятельствами совершенного уголовного правонарушения;

– сведения об известных обстоятельствах и возможных причинах совершенного уголовного правонарушения;

– данные о лицах, которые, предположительно, могли совершить данное уголовное правонарушение.

При **допросе специалиста, эксперта** выясняется вся юридически значимая и важная для установления истины по делу информация, ставшая им известной в ходе и по результатам проведенных исследований.

В том числе, важно выяснить следующие обстоятельства:

– действительно ли имело место событие уголовного правонарушения, указанное потерпевшим;

– имеются ли в совершенном деянии все признаки, соответствующие признакам соответствующего состава уголовного правонарушения;

– причинен ли фактически ущерб потерпевшему от данного уголовного правонарушения;

– соответствует ли характер и размер причиненного уголовным правонарушением вреда заявленному потерпевшим.

При **допросе подозреваемого** необходимо тщательно выяснить все обстоятельства, входящие в предмет доказывания по делу (*см. л. 12 «настоящих методических рекомендаций*).

После определения времени и места допроса, дознаватель приступает к изучению личности допрашиваемого. Данные о личности допрашиваемого связаны с его психофизиологическими свойствами и состоянием, общественно–политической и трудовой деятельностью, отношением к коллективу и коллектива к нему, моральным обликом и поведением в быту, отношением к другим, проходящим по делу.

Полученные сведения позволяют дознавателю (следователю) сформулировать мнение о допрашиваемом лице и выбрать наиболее продуктивную тактику проведения допроса.

3.4. Особенности изъятия криптовалют при досудебном расследовании уголовных правонарушений

Криптовалюта – цифровая расчетная единица, имеющая материальную ценность, определяемую биржевыми котировками в странах, имеющих правовой режим их эмиссии (выпуска) и обращения.

Формы существования (хранения, фактического нахождения) криптовалют (электронных ресурсов доступа и распоряжения):

1) на материальном электронном носителе информации (*флэш-карта, жесткий диск компьютера, CD-диск и т.д.*);

2) на виртуальном электронном носителе информации (*персональный электронный кошелек, хранящийся в «облачном» информационном поле; персональный электронный счет на криптобирже, функционирующей на базе виртуальных (облачных) информационных технологий*);

при этом в юрисдикции Республики Казахстан официальное хранение криптовалюты и официальные транзакции с ней посредством виртуальных электронных носителей информации легально не осуществляется, ввиду отсутствия соответствующего правового режима (*но осуществляется в юрисдикции и на территории иностранных государств, в которых криптовалюта имеет официальный правовой режим, либо в нелегальном интернет-пространстве «Даркнете»*).

Материальная ценность криптовалюты в Республике Казахстан обусловлена тем, что криптовалюта может быть обменена на деньги, в том числе по официальному обменному курсу (*в стране с официальным правовым режимом этой криптовалюты*), а также может использоваться как электронное платежное средство в обмен на товары и услуги, приобретаемые на интернет-ресурсах (*т.е. фактически используется в торговом обороте*).

Отсутствие правового режима криптовалют в Республике Казахстан не исключает фактического ее оборота на территории Республики Казахстан.

Соответственно, криптовалюта в Республике Казахстан обладает всеми признаками легального имущества:

1) наличие фактической материальной ценности криптовалюты;

2) способность криптовалюты принадлежать определенному физическому или юридическому лицу; возможность фактического перехода от одного обладателя к другому;

3) возможность фактического использования и распоряжения ею на территории страны;

4) отсутствие юридического запрета к ее свободному обороту в Республике.

В свою очередь, отсутствие специального правового статуса и правового режима криптовалюты по законодательству Республики Казахстан не препятствует признанию криптовалюты имуществом на территории Республики Казахстан.

Признание криптовалюты имуществом позволяет следственным органам на общих основаниях совершать в отношении криптовалюты (электронных ресурсов доступа и распоряжения) следственные и иные процессуальные действия (*осмотр, изъятие, выемка, назначение экспертизы и др.*).

Идентификация криптовалюты (определение ее вида, наименования), установление ее истинной материальной ценности может быть осуществлено только посредством специальной экспертизы или заключения специалиста. Для этого *следственным органам необходим полный доступ к изымаемой криптовалюте (электронным ресурсам доступа и распоряжения)* (*т.е. прямой доступ к каждой криптоманете, представляющей собой электронную запись в виде набора электронных символов*).

Соответственно, *на момент изъятия криптовалюты речь может идти только об изъятии самого материального носителя информации, на котором предположительно содержится криптовалюта (электронный ресурс доступа и распоряжения)* (*флэш-карта, жесткий диск компьютера, CD-диск и т.д.*).

При этом все процессуальные действия (осмотр, изъятие, выемка) в отношении критовалюты (*или электронных ресурсов доступа и распоряжения*) должны осуществляться с привлечением специалистов в области работы с компьютерной информацией и ее носителями, а также в сфере криптографии и электронных платежных средств и систем.

Совершение процессуальных действий в виртуальном пространстве (*арест виртуальных электронных криптосчетов, изъятие криптовалюты в виртуальных информационных системах*) *не представляется возможным, прежде всего, из-за отсутствия правового режима криптовалют в Республике Казахстан*.

Таким образом, *вопрос изъятия криптовалюты* (носителей информации, на которых предположительно содержится криптовалюта) *может быть решен в следующих случаях*:

1) криптовалюта (электронный ресурс доступа и распоряжения) обнаружена на материальном электронном носителе информации (*на флэш-карте, CD-диске, жестком диске компьютера*) на территории Республики Казахстан и имеются пароли, шифры к разблокировке данных носителей;

2) если лицо, владеющее электронным кошельком или электронным счетом (*что возможно только в иностранной юрисдикции*) самостоятельно переведет криптовалюту на материальный носитель (*флэш-карта, жесткий диск компьютера, CD-диск и т.д.*) и выдаст следственным органам.

3) по запросу в правоохранительный орган государства, в юрисдикции которого находится соответствующий электронный кошелек или счет, в порядке взаимодействия и оказания правовой помощи по уголовным делам на основании международных договоров Республики Казахстан.

Вероятность получения следственными органами Республики Казахстан доступа к криптовалюте, хранящейся на виртуальном электронном носителе информации (*электронный криптокошелек, электронный счет криптобиржи*) *крайне низка* по следующим причинам:

1) владелец (*фактический обладатель*) криптовалюты, как правило, самостоятельно не выдает криптовалюту и не указывает доступ к ней, ссылаясь на утрату соответствующих паролей и шифров;

2) организации, содержащие и администрирующие хранение и оборот криптовалюты в виртуальных информационных системах, зачастую имеют сложную организационно-правовую форму с регистрацией в отдаленных, труднодоступных юрисдикциях либо действуют нелегально (*без юридической регистрации*) (*например в нелегальном интернет-пространстве «Даркнете»*);

3) каналы международного сотрудничества правоохранительных органов на сегодняшний день не эффективны в виду недостаточного правового регулирования отношений, связанных с эмиссией и оборотом криптовалют.