

увеличилось в сравнении с довоенным периодом, что подчеркивает важное значение, уделяемое этому вопросу руководством НКВД.

### Список источников

1. Архив УМВД России по Приморскому краю
2. Архив УМВД России по Хабаровскому краю
3. Милежик А. В. Деятельность Центральной школы подготовки комсостава народной милиции ДВР: опыт организации профессионального образования на Дальнем Востоке России // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. 2018. № 2 (44). С. 135–145.
4. Худяков П. П., Швец А. В. Становление и развитие организационно-правовых основ и структуры аппарата милиции Приамурья (1917–1982 гг.). Благовещенск, 2008. 208 с.
5. Шабельникова Н. А. На страже правопорядка: история органов внутренних дел России в современной дальневосточной историографии // Клио. 2020. № 5 (161). С. 20–27.
6. Шабельникова Н. А., Бакшуттов С. Н. Формирование системы профессионального обучения кадров милиции на Дальнем Востоке России в 1920-е гг. // Теория и практика общественного развития. 2015. № 21. С. 182–185.

УДК 343.98

## ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

*П. А. Жердев, доцент кафедры криминалистики Дальневосточного юридического института МВД России, кандидат юридических наук*

Вопросы, посвященные преступности в сфере информационной безопасности, настоятельно требуют более конкретного теоретического осмысления и изучения. В настоящем исследовании предлагается авторское решение некоторых малоизученных вопросов, касающихся данной проблемы.

**Ключевые слова:** электронная информация, неправомерный доступ, компьютерная техника, программное средство.

## FEATURES OF THE INITIAL STAGE OF THE INVESTIGATION OF CRIMES RELATED TO ILLEGAL ACCESS TO COMPUTER INFORMATION

*P.A. Zherdev, chair associate professor of the Far Eastern Law Institute of the Ministry of Internal Affairs of Russia, kandidat nauk, degree in Law*

The issues related to crime in the field of information security urgently require a more specific theoretical understanding and study. This study offers the author's solution to some little-studied issues related to this problem.

**Keywords:** electronic information, unauthorized access, computer equipment, software tool.

Одним из необходимых элементов объекта криминалистической науки является деятельность органов предварительного расследования по раскрытию и расследованию преступлений. Эффективность расследования напрямую зависит от рациональной организации предварительного расследования. Еще А. М. Ларин писал: «... организация расследования – это рациональный выбор, расстановка и приложение сил, орудий и средств, которыми располагает следователь, создание и использование оптимальных условий для достижения целей правосудия» [5, с. 59].

Организация предварительного расследования уголовного дела осуществимо в определенной обстановке, которая проявляется в определенное время и в конкретном месте и закономерно оказывает на них значительное влияние, и напрямую зависит от складывающейся по уголовному делу следственной ситуации, что обязательно приводит к ситуационному характеру процесса расследования, которая положена в основу частной криминалистической теории о криминалистических (следственных) ситуациях.

Р. З. Емалетдинов считает, что криминальная ситуация должна отражать один из важных элементов криминалистической характеристики преступления – обстановку (условия) совершения преступления [3, с. 3]. При этом криминальные ситуации могут формироваться не только на этапе подготовки к совершению преступления, но и на этапах его совершения или же сокрытия.

Отечественная криминалистика на протяжении длительного времени уделяет внимание на сущность и содержание криминалистической ситуации. Так, профессор кафедры специальных юридических дисциплин Т. С. Волчецкая сформулировала целостную теорию криминалистических ситуаций, разработала методические основы познания, исследования, типизации и разрешения различных видов криминалистических ситуаций [1, с. 248]. Это исследова-

ние дало толчок к исследованию проблем различных ситуаций (следственных, оперативно-розыскных, экспертных и судебных). Представляется, что из перечисленных наиболее криминалистически важной является следственная ситуация.

С. Н. Чурилов под следственной ситуацией понимает совокупность обстоятельств и условий, которые создают обстановку, в которых предстоит или приходится осуществлять расследование уголовного дела [8, с. 52].

С. А. Куемжиева считает под следственной ситуацией совокупность значимой для расследования информации, которая существует в определенный момент расследования уголовного дела, а также возможность следователя квалифицированно провести расследование уголовного дела [4, с. 191]. Представляется, что информация может быть разной: информация, которая прошла проверку процессуальным путем (доказательства) и информация, которая носит ориентировочный характер и которая может преобразоваться в доказательственную путем проведения следственных действий. А в целом, нам следственная ситуация представляется системой условий и обстоятельств, которые характеризуют состояние расследования уголовного дела на определенный момент, а также обстановку, в которой действует следователь.

У криминалистов нет единого мнения по поводу следственной ситуации. А. Г. Филиппов и А. Я. Целищев под следственной ситуацией понимали «сумму значимой для расследования информации (доказательств и сведений, полученных не процессуальным путем)», которая имеется к конкретному моменту в распоряжении следователя [7, с. 71]. В данном определении нам непонятно, почему информация и сведения должны получаться исключительно непроцессуальным путем.

Типовые следственные ситуации могут разными в зависимости от вида совершенного преступления. При расследовании преступлений, связанных с неправомерным доступом к компьютерной информации типовыми следственными ситуациями, могут быть:

- следственные ситуации, в которых сообщение о преступлении и материалы, которые приложены к сообщению, достаточны для возбуждения уголовного дела;

- следственные ситуации, в которых сообщение о преступлении и материалы, которые приложены к сообщению, содержат сведения о противоправных действия, однако недостаточны для возбуждения уголовного дела.

К первой следственной ситуации можно отнести такую ситуацию, когда потерпевший сам выявил факт преступлений, связанный с неправомерным доступом к компьютерной информации. Естественно, такая ситуация наиболее благоприятна для расследования такого преступления.

Ко второй ситуации, относится факт, когда неправомерный доступ обнаружен при реализации компьютерной информации незаконным пользователем (например, при осуществлении передачи логина и пароля в сети Интернет). Сюда же относится ситуация, когда неправомерный доступ обнаружен в результате того, что лицо, осуществляющее такой доступ, застигнуто на месте преступления.

Следственная ситуация третьего типа, возникает тогда, когда имел место неправомерный доступ к компьютерной информации, однако лицо его совершившее, не установлено и на этапе проверки сообщения о преступлении нет возможности установить его.

В любом случае независимо от возникшей ситуации при неправомерном доступе к компьютерной информации на первоначальном этапе расследования с целью раскрытия преступления «по горячим следам» следователь (или сотрудник оперативного подразделения по его поручению) осуществляет комплекс первоочередных мероприятий, в частности:

- допрашивает потерпевшего и возможных свидетелей, которым могут быть известны обстоятельства, имеющие значение для уголовного производства;
- проводит осмотр компьютера, смартфона или другого средства с выходом в сеть Интернет пострадавшего;

- проверяет все аналогичные случаи завладения компьютерной информацией граждан (аналогичным способом, в конкретном районе, в одинаковое время), лиц, состоящих на соответствующих учетах, а также лиц, в отношении которых получена оперативная информация об их возможной причастности к преступлению;

- обращается в суд с ходатайством о предоставлении временного доступа к информации о звонках подозреваемого, обязав операторов мобильной связи распечатать на бумажном и электронном носителе документ с указанными абонентскими номерами и периодом времени;

- использует возможности оперативно-технической службы, информационно-поисковых систем полиции, а также информационных ресурсов других организаций, средств массовой информации и частных лиц.

Таким образом, каждой из перечисленных типовых следственных ситуаций присущ определенный алгоритм действий, который обусловлен совокупностью конкретных обстоятельств.

Поскольку преступники, как правило, совершают не одно преступление, а серию однотипных хакерских атак, для оперативного реагирования, своевременного раскрытия и качественного расследования преступлений указанной категории необходимо надлежащее взаимодействие между подразделениями и службами органов полиции в ходе расследования, а также создание специализированных следственно-оперативных групп для осуществления производств указанной категории.

В зависимости от сложившихся следственных ситуаций на первоначальном этапе расследования могут быть сформулированы следующие версии:

- совершенное преступление, связанное с неправомерным доступом к компьютерной информации, действительно имеет место при обстоятельствах, изложенных потерпевшим;

- преступление с использованием сети Интернет не имело место, потерпевший добросовестно заблуждается относительно действий другого лица;

- неправомерного доступа к компьютерной информации нет, совершено другое преступление.

Один из наиболее важных вопросов, стоящих перед следователем при расследовании преступлений, совершенных посредством неправомерного доступа в корпоративную сеть, – установление возможной причастности работников потерпевшей организации либо иных лиц, которые в силу своих служебных обязанностей имеют доступ к ее конфиденциальной информации и возможность подключения к корпоративной сети. Сложность разрешения этого вопроса усугубляется тем, что современные комплексы вредоносного программного обеспечения обладают настолько мощным инструментарием, обеспечивающим проникновение даже в хорошо защищенные локальные сети, что создается ложное впечатление о невозможности проведения такой атаки без привлечения инсайдера.

Вместе с тем, выявление вредоносных программ и следов их работы на компьютерах и серверах корпоративной сети не может считаться безусловным аргументом, чтобы не рассматривать версию совершения преступления работником пострадавшей организации, тем более при планировании и производстве первоначальных следственных действий. Результаты проведенной впоследствии судебной компьютерной экспертизы могут установить отсутствие причинно-следственной связи между выявленным вредоносным программным обеспечением и несанкционированным списанием финансовых средств, но к этому времени возможность отыскания новых доказательств на месте происшествия, например, следов рук на клавиатуре терминала банковского процессинга, с которого была отдана команда на выдачу денег банкоматами, будет безвозвратно утрачена.

При таких обстоятельствах, приступая к расследованию преступлений, связанных с неправомерным доступом в корпоративную компьютерную сеть, к внутренним сетевым ресурсам и сервисам организаций, необходимо рассматривать обе версии:

- преступление связано с несанкционированным проникновением в корпоративную компьютерную сеть в результате эксплуатации уязвимостей программного обеспечения, ошибок сетевых настроек и/или с применением вредоносных программ;

– преступление совершено работником организации, воспользовавшимся физическим доступом к компьютерам и серверам корпоративной сети.

Планируя допрос потерпевшего, следователю (сотруднику уголовного розыска) целесообразно выяснить такой круг вопросов:

– каким способом совершено преступление (в каком месте, в какое время и т. д.);

– каким образом преступник завладел конфиденциальной информацией (логинами и паролями к сайтам, серверам и иным электронным хранилищам);

– если состоялась встреча, то необходимо выяснить характеристику лица, с которым встречался потерпевший (пол, возраст, одежда, голос, национальность, цвет волос, глаз, кожи, особые приметы, повторяющиеся часто слова в речи, манера разговора);

– установить все технические средства связи и программное обеспечение потерпевшего и подозреваемого;

– определить персональный (заводской) номер (IMEI) и абонентский номер смартфона потерпевшего;

– кто, по мнению потерпевшего, может быть причастен к такому преступлению.

Временный доступ к конфиденциальным документам осуществляется на основании решения суда и постановления следователя [2, с. 35]. У операторов и провайдеров телекоммуникационной сети, следователь может получить информацию:

– о виде связи, абоненте, предоставлении Интернет услуг, их длительности, содержания, маршрутов передачи и тому подобное;

– об идентификационных признаках конечного оборудования (IP-адрес компьютера, абонентский номер, SIM-карты и др.);

– о месте пребывания в прошлом идентифицированного конечного оборудования телекоммуникаций (по азимуту) в зоне действия определенных базовых станций в определенное время или его промежутков;

– фамилия, имя, отчество и другие сведения об абонентах телекоммуникационных услуг;

– маршруты переданной информации независимо от вида телекоммуникационной сети;

– выходное соединение – номер стороны, с которой связывались, даже если связь не была установлена;

– входное соединение – номер стороны, которая связывалась, даже если связь не была установлена;

– начало, конец и продолжительность соединения, которое произошло без раскрытия содержания передаваемой информации;

– о фактическом месте назначения и промежуточный абонентский номер в случае, если связь была переадресована.

Полученная информация может быть использована по нескольким направлениям:

Во-первых, поиск подозреваемого по IP-адресу или по абонентскому номеру смартфона. Если терминал, с которого осуществлялся неправомерный доступ, продолжает работать, по полученным от оператора мобильной связи трафиками (распечатками телефонных соединений) возможно установить номера смартфонов, с которыми соединялся абонент. Также от оператора можно получить информацию о размещении базовых станций, в зоне действия, которых он работает.

Во-вторых, поиск подозреваемого по номеру IP-адреса компьютера. IP-адрес является уникальным сетевым адресом узла в компьютерной сети, которые построен на основе стека протоколов TCP/IP и на котором функционирует сеть Интернет, и IP-адреса узла сети или технологии. При этом номер сети Интернет в последующих подключениях, как правило, совпадает у разных устройств, что свидетельствует о территориальной близости друг к другу точек доступа [6, с. 85].

Таким образом, на первоначальном этапе расследования преступлений, связанных с неправомерным доступом к компьютерной информации, совершенных с использованием сети Интернет типовыми следственными ситуациями может быть обстановка, в которой сообщение о преступлении и прилагаемые результаты предварительной проверки достаточны для возбуждения уголовного дела и следственные ситуации, в которых сообщение о преступлении и предоставляемые материалы, которые приложены к сообщению, содержат сведения о противоправных действиях, однако недостаточны для возбуждения уголовного дела.

#### **Список источников:**

1. Волчечкая Т. С. Криминалистическая ситуалогия: монография / под ред. проф. Н. П. Яблокова. Калининград, 1997. С. 248.
2. Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий. 2018. № 4. С. 35
3. Емалетдинов Р. З. Структура криминалистической характеристики незаконного пересечения государственной границы Российской Федерации // Российский следователь. 2013. № 7. С. 3–6.
4. Кумежиева С. А. Понятие следственной ситуации и ее роль в определении средств и методов отдельного расследования // Вестник Краснодарского университета МВД России. 2015. № 4 (30). С. 191–195.

5. Ларин А. М. Расследование по уголовному делу. Планирование, организация. М., 1970. С. 59–67.
6. Сидорова К. С. IP-адрес как один из идентификаторов личности в расследовании преступлений // Психопедагогика в правоохранительных органах. 2018. № 3(74). С. 84–87.
7. Филиппов А. Г., Целищев А. Я. Узловые проблемы методики расследования преступлений // Советское государство и право. 1982. № 8. С. 71.
8. Чурилов С. Н. О некоторых уточнениях понятия «следственная ситуация» и его отношениях со смежными криминалистическими понятиями // Вестник Московского городского педагогического университета. Серия: Юридические науки. 2018. № 2 (30). С. 52–58.

УДК 343.98

## О ХАРАКТЕРИСТИКЕ ЛИЧНОСТИ НЕСОВЕРШЕННОЛЕТНЕГО ПРЕСТУПНИКА И ЕЕ ЗНАЧЕНИИ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ОТДЕЛЬНОГО ВИДА

*Е. В. Жидкова, старший преподаватель кафедры криминалистики и специальной техники Владивостокского филиала Дальневосточного юридического института МВД России*

Статья посвящена отдельным аспектам расследования преступлений, совершенных несовершеннолетними, криминалистической характеристика преступления, рассмотрена характеристика личности несовершеннолетнего преступника как элемента криминалистической характеристики. Сделан вывод о необходимости развернутого исследования личности несовершеннолетнего преступника в целях успешного расследования.

**Ключевые слова:** криминалистическая методика, криминалистическая характеристика преступления, характеристика личности несовершеннолетнего преступника, расследование преступлений.