ISBN 978-5-901722-00-8
5 [2025]
ТРАНСПОРТ. ГОРИЗОНТЫ РАЗВИТИЯ

УДК 347.9

ПЕРВОНАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Щеголева Ксения Вячеславовна[1], магистрант
e-mail: rctybz19991@mail.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия

Аннотация. В статье исследуется многогранная и постоянно эволюционирующая проблема борьбы с преступлениями в сфере компьютерной информации. Теоретическая глубина и практическая значимость вопросов, возникающих в процессе расследования киберпреступлений, закономерно привлекают пристальное внимание как российских, так и зарубежных ученых. Способы совершения преступлений в цифровом пространстве становятся все более изощренными и непредсказуемыми. В этой динамичной среде теоретики и практики обязаны неустанно отслеживать новые тенденции и разрабатывать инновационные стратегии противодействия, опережая преступников на шаг.

Ключевые слова: «киберпреступность», преступления, компьютерная информация, системы ЭВМ, компьютерная преступность.

THE INITIAL STAGE OF INVESTIGATION OF CRIMES IN THE FIELD OF COMPUTER INFORMATION

Ksenia V. Shchegoleva[1], Master's Degree Student
e-mail: rctybz19991@mail.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia

Abstract. The article explores the multifaceted and constantly evolving problem of combating crimes in the field of computer information. The theoretical depth and practical significance of the issues arising in the investigation of cybercrimes naturally attract the close attention of both Russian and foreign scientists. The ways of committing crimes in the digital space are becoming more sophisticated and unpredictable. In this dynamic environment, theorists and practitioners are required to tirelessly monitor new trends and develop innovative counteraction strategies, one step ahead of criminals.

Keywords: «cybercrime», crimes, computer information, computer systems, computer crime.

Бурное развитие компьютерной техники и средств телекоммуникаций способствует возникновению киберпреступности, что оказывает влияние на практически все сферы человеческой деятельности.

Различные термины, такие как «преступления в сфере компьютерной информации», «киберпреступность» и «компьютерные преступления», используются взаимозаменяемо, вызывая много дискуссий из-за различных подходов к их определению.

При расследовании компьютерных преступлений важно определить обстоятельства, которые могут послужить основой для постановки задач расследования.

Признаки несанкционированного доступа могут включать в себя появление фальшивых данных, не обновление кодов и паролей, частые сбои в работе компьютеров, участившиеся жалобы клиентов и другие явные признаки.

Важно учитывать общий перечень обстоятельств, подлежащих доказыванию согласно уголовно-процессуальному кодексу РФ [1].

Согласно статье 272 УК РФ, неправомерный доступ к компьютерной информации может повлечь за собой ее уничтожение, блокирование, модификацию или копирование

Раскрытие преступлений, связанных с незаконным доступом к компьютерной информации (ст. 272 УК РФ), требует особого внимания к мотивации злоумышленника. Ключевым моментом является установление цели: направлен ли преступный акт на охраняемую законом информацию, хранящуюся в компьютерных системах, сетях или на носителях, а также передаваемую через компьютерные сети? Необходимо проследить прямую причинно-следственную связь между действиями преступника и возникшими последствиями: уничтожением, блокировкой, изменением или копированием данных, нарушением работы компьютеров, систем или сетей.

В расследовании преступлений, связанных с вредоносными программами, crucial доказать осознанное использование их как инструмента для несанкционированного доступа, уничтожения, блокировки, изменения или копирования информации, а также для нарушения работоспособности систем. При этом, особое внимание следует уделить процессу создания самих программ, отдельных их компонентов, подпрограмм и модулей.

Исследуя преступления, обусловленные нарушениями правил эксплуатации компьютерных систем, важно установить наличие квалифицированного субъекта – лица, имеющего доступ к ЭВМ, системе ЭВМ или сети [2]. Ключевым является доказательство причинения существенного вреда в результате неправомерных действий. Как отмечает Е.П. Ищенко, без такого вреда уголовная ответственность не наступает.

Рекомендации для улучшения: Уточнить «материалы следы компьютерных преступлений». Что конкретно подразумевается? Логические следы (журнал событий, файлы), физические следы (компьютер, периферия), электронные следы (переписки, траффик)? Подробности помогут читателю лучше понять практический смысл.

Добавить конкретные примеры способов совершения преступлений, которые усложняются. Например, «Фишинг с использованием глубокого обучения для подделки голосов», «атаки на цепочки поставок программного обеспечения», «использование криптографии для анонимизации действий». Это сделает текст более практичным и убедительным.

Указать на роль экспертизы. Поскольку киберпреступления часто требуют специализированных знаний, важно подчеркнуть необходимость привлечения экспертов-компьютерщиков, криптографов, аналитиков данных, и так далее.

Рассмотреть аспекты международного сотрудничества. Киберпреступления часто имеют трансграничный характер, поэтому важно указать на необходимость сотрудничества между правоохранительными органами разных стран [3].

Обсудить этические и правовые аспекты. Следует упомянуть о важности соблюдения прав и свобод граждан в процессе расследования киберпреступлений, а также о необходимости соблюдения правовых норм при работе с киберданными.

В целом, текст хорошо структурирован и содержит важные мысли. Добавление конкретики и углубление некоторых аспектов позволит сделать его ещё более полезным для аудитории.

Из приведенного текста можно выделить типичные следственные ситуации на первоначальном этапе расследования, хотя сам текст не описывает их конкретно. Логически можно предположить, что такие ситуации будут складываться из элементов, указанных авторами [4]:

Типичные следственные ситуации первоначального этапа расследования (предполагаемые) [7]:

Ситуация недостаточной информации:

– отсутствие очевидцев или свидетелей;
– недостаточно полное описание преступления;
– нет явных улик или следов преступления;
– неясно, кто совершил преступление;
– неясны мотив и цель преступления.

Ситуация противоречивой информации:

– разноречивые показания свидетелей;
– противоречия в собранных фактах и доказательствах;
– низкая достоверность имеющейся информации;
– возможная фальсификация информации.

Ситуация «горячих следов»:

– недавно совершенное преступление, с неидентифицированным преступником;
– наличие свежих следов преступления (отпечатков пальцев, ДНК, отходов) ;
– возможность оперативного задержания преступника на месте преступления или вблизи него.

Ситуация предполагаемого совершения преступления лицом, имеющим алиби:

– необходимо подтверждение или опровержение алиби;
– проверка логики и возможности совершения преступления с учётом алиби.

Ситуация наличия подозреваемого (подозрения):

– идентифицирован подозреваемый;
– необходима проверка обоснованности подозрений;
– поиск дополнительных доказательств;
– возможность допроса подозреваемого.

Ситуация «встречных» действий, направленных на сокрытие преступления:

– предполагаемое сокрытие следов преступления или уничтожение улик;
– наличие противодействия следствию со стороны окружающих;
– необходимость быстрой и эффективной реакции на сокрытие.

Ситуация сложной географической локализации преступления:

– преступление совершено в труднодоступном или удаленном месте;
– преступление совершено в нескольких местах;
– сложности с получением информации и улик.

Важное замечание: Эти ситуации не являются взаимоисключающими. В реальном расследовании часто встречаются комбинации нескольких ситуаций, которые могут динамически меняться по мере продвижения следствия. Следователь должен уметь распознавать и адаптировать свою тактику в соответствии с конкретной сложившейся следственной ситуацией [5].

На начальной стадии расследования киберпреступлений часто встречаются следующие сценарии:

а) Если владелец или пользователь компьютерных данных самостоятельно обнаружил факт правонарушения и установил личность виновного [7], то обычно проводятся:

1) задержание подозреваемого лица;

2) проведение допроса с подозреваемым;

3) производство обысков в жилище и на рабочем месте подозреваемого или других лиц, где могут находиться предметы, имеющие значение для расследования;

4) обследование места инцидента;

5) изучение конфискованных носителей данных;

6) допрос свидетелей;

7) назначение судебных экспертиз для анализа;

8) проведение следственного эксперимента.

б) Если собственник информации самостоятельно выявил преступление, но личность злоумышленника не установлена, то характерны следующие действия:

1) допрос заявителя;

2) Признание собственника потерпевшей стороной;

3) осмотр места совершения преступления;

4) поручение органам, осуществляющим оперативно-розыскную деятельность, задачу по поиску преступников и установлению обстоятельств, имеющих значение для дела;

5) допрос свидетелей для получения информации;

6) анализ ситуации и разработка версий относительно каждого аспекта, требующего выяснения;

7) назначение необходимых экспертиз;

8) установление личности преступника и его задержание.

в) Если преступление выявлено органом дознания в ходе оперативно-розыскных мероприятий, то, как правило, проводятся [6]:

1) осмотр места преступления для фиксации обстановки;

2) допрос свидетелей для получения информации об обстоятельствах дела;

3) обыск с конфискацией документов и носителей информации;

4) проведение следственного эксперимента для проверки версий;

5) прослушивание телефонных переговоров (при наличии санкции);

6) назначение судебных экспертиз для анализа собранных данных [8].

Исходя из сложившейся ситуации, разрабатывается план расследования, охватывающий дело в целом, отдельные эпизоды и обстоятельства. Важно подчеркнуть, что целенаправленные действия сотрудников правоохранительных органов, особенно на начальном этапе расследования компьютерных преступлений, являются залогом успешного раскрытия уголовного дела.

Список литературы:

1. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: от 18 декабря 2001 г. № 174-ФЗ: (в ред. от 7 июня 2017 г.) // Консультант Плюс: справ. правовая система. Версия Проф. Электрон. дан. М., 2020.

2. Уголовный кодекс Российской Федерации [Электронный ресурс]: от 13 июня 1996 г. № 63-ФЗ.

3. Ищенко Е. П., Топорков А. А. Криминалистика. М., 2005. С. 733.

4. Колесниченко Д. Н. Научные и правовые основы методики расследования отдельных видов преступлений: дис. д-ра юрид. наук. Харьков, 1967. С. 10.

5. Драпкин Л. Я. Основы теории следственных ситуаций. Свердловск, 1987. С. 17.

6. Белкин Р. С. Курс криминалистики. М., 1997. Т. 2 С. 135.

7. Подольный Н. А. Отдельные проблемы расследования преступлений, совершённых с применением компьютерных технологий // Библиотека криминалиста. Научный журнал. 2013. № 5 (10). С. 117.

8. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. М. : Юрид. лит., 1991. – 157 с.