Максюта Екатерина Александровна,
Студент бакалавр юридического факультета,
Российский государственный социальный университет,
г. Москва, Российская Федерация

Maksyuta Ekaterina Alexandrovna,
,
The student of the bachelor of law faculty
Russian State Social University,
Moscow, Russian Federation

РАССЛЕДОВАНИЕ И РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ.

Investigation and disclosure of crimes in the field of high technologies

Аннотация: статья посвящена исследованию проблемы преступлений в сфере высоких технологий и, в частности, механизма их совершения и организационно-технических и правовых механизмов их предупреждения, расследования и раскрытия. Статья адресована сотрудникам следственных органов, а также сотрудникам судебно-экспертных подразделений (судебным экспертам в области технико-криминалистической экспертизы документов).

Ключевые слова: сфера высоких технологий; уголовный кодекс; методы расследования и раскрытия преступлений

Abstract: The article investigates the problem of crime in the sphere of high technology and, in particular, the mechanism of their occurrence and the organizational, technical and legal mechanisms for their prevention, investigation and disclosure. The article is addressed to employees of the investigating authorities, as well as employees of forensic units (forensic experts in the field of technical and forensic examination of documents).

Keywords: the sphere of high technologies; Criminal Code; methods of investigating and solving crimes

Глава 28 Уголовного кодекса Российской Федерации закрепляет ответственность за преступления в сфере компьютерной информации.
Следователи и дознаватели констатируют, что им все чаще приходится расследовать следующие киберпреступления, предусмотренные УК РФ:

- ст. 159.6 - «Мошенничество в сфере компьютерной информации»,
- ст. 242.1 - «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»,
- ст. 273 - «Создание, использование и распространение вредоносных компьютерных программ», ст. 242 - «Незаконные изготовление и оборот порнографических материалов или предметов",
- ст. 274 - «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации информационно-телекоммуникационных сетей»,
- ст. 158 - «Кража»,
- ст. 183 - «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»,
- ст. 138 - «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»,
- ст. 272 - «Неправомерный доступ к компьютерной информации»,
- ст. 137 «Нарушение неприкосновенности частной жизни»,
- ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».

Общественная опасность данной группы преступлений достаточно высока, о чём свидетельствуют опубликованные МВД России статистические данные: в 2011 году было зарегистрировано 2698 подобного рода преступлений, 2012 году – 2820. Таким образом, рост «компьютерной» преступности за указанный период составил около 4,5 %.

Цифры показывают, что компетентность занимающихся расследованием кибепреступлений недостаточная

Ключевая проблема, которые выделяют исследователи, заключается в недостаточной компетентности лиц, занимающихся выявлением и раскрытием киберпреступлений. Опросы среди следователей показывают, что 95% респондентов получили юридическое образование. И только 5% обладают еще и образованием по специальности «Информатика и вычислительная техника». 63% опрошенных владеют компьютером на уровне «среднего пользователя», 37% - на уровне «продвинутого пользователя». 79% при этом постигают компьютер самостоятельно, курсы

для сотрудников правоохранительных органов посещали только 21%, и незначительный процент (5%) - коммерческие курсы.

Кибепреступления на шаг впереди следователей

Другой проблемой является несвоевременность выявления киберпреступлений.

В соответствии с результатами опросов:

- в 53% случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней;
- 73% респондентов отметили запоздалое начало предварительного расследования, когда многие важные доказательства уже утрачены.

Какие действия проводят на месте расследования преступлений?

- осмотр, об этом сказали 79%;
- допрос, об этом сказали 68%;
- обыск, об этом сказали 63%,
- назначение судебных экспертиз, об этом сказали 47%,
- выемка, об этом сказали 37%.

С чем возникают трудности?

Наибольшие трудности возникают при проведении осмотра места происшествия и назначении судебных экспертиз.

При этом многие респонденты отмечали, что и вовсе не проводили осмотр места происшествия. Причина проста – оно отсутствует. Это значит, что распознавание места совершения киберпреступления невозможно без установления обстановки совершения преступления, которая определяется системой киберпространства.

Для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания. И начать надо с определения единого понятия киберпространства с точки зрения криминалистики.

А что касается назначения компьютерно-технической экспертизы?

Следователи отмечают высокую загруженность государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз. А ведь в 58% случаев проведение экспертизы они поручали государственно-экспертным учреждениям и лишь в 5% - негосударственным.

Немаловажной проблемой при назначении экспертиз является **постановка грамотных вопросов эксперту**. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики

расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере.

В качестве вывода

Раскрытие и расследование киберпреступлений остается довольно сложной задачей для большинства сотрудников органов предварительного расследования. Это обусловлено:

- отсутствием системных обобщений материалов следственной и судебной практики,
- нехваткой методических рекомендаций по организации расследования данного вида преступлений,
- небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов,
- недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Для решения приведенных проблем ученые и представители профсообщества рекомендуют:

- повысить уровень мониторинга данного вида преступлений;
- разработать программы повышения квалификации следователей (дознавателей) по расследованию данной категории дел;
- повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий;
- увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования киберпреступлений.

Список литературы:

1. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис. ... канд. юрид. наук / Ижевск, 2002.
2. Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. ... докт. юрид. наук. М., 2007.
3. Лузгин И.И. Технико-криминалистическое обеспечение как мегаинструментальная технология формирования единого криминалистического пространства // Эксперт-криминалист. 2010. N 1. С. 30 - 33.
4. Лысов Н.Н., Салтевский М.В. Новый подход в технологии собирания и исследования информационных следов // Эксперт-криминалист. 2008. N 1. С. 16 - 19.
5. Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий: дис. ... канд. юрид. наук. Краснодар, 2009.

6. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. ... канд. юрид. наук. М., 2005.
7. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: дис. ... канд. юрид. наук. Красноярск, 2010.
8. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток, 2005.
9. Никодимов И.Ю. НЕКОТОРЫЕ ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ТАМОЖЕННОГО ЗАКОНОДАТЕЛЬСТВА С ТОЧКИ ЗРЕНИЯ ОПЕРАТОРОВ МОБИЛЬНОЙ СВЯЗИ В книге: Роль таможенной службы в условиях переходного периода. Тезисы докладов международной научно-практической конференции. Северо-Западное таможенное управление Российской Федерации; Санкт-Петербургский им. В. Б. Бобкова филиал Российской таможенной академии. 1999. С. 179-182.
10. Никодимов И.Ю., Бабешко Е.В. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СФЕРЕ ОБРАЗОВАНИЯ В сборнике: Проблемы назначения и исполнения наказания и мер уголовно-правового характера. Сборник статей. Под редакцией В.Ю. Голубовского. Москва, 2018. С. 205-211
11. Нуждин К.С., Никодимов И.Ю. ОБРАБОТКА ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ КАК СПОСОБ ЗАЩИТЫ ЧЕСТИ, ДОСТОИНСТВА И ДЕЛОВОЙ РЕПУТАЦИИ В сборнике: УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ И НАКАЗАНИЕ.ОПЫТ РОССИИ И ЗАРУБЕЖНЫХ СТРАН. сборник статей по материалам научно-практической конференции. 2019. С. 167-170.
12. Климантова Е.Д., Никодимов И.Ю. МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В сборнике: Противодействие преступности в сфере высоких технологий. Сборник статей по материалам конференции. Под редакцией В.Ю. Голубовского. 2020. С. 73-85