УДК 343.98.067

В.В. Григорьев

Студент 4 курса Института правоохранительной деятельности

ФГБОУ ВО «СГЮА»

Саратов

Научный руководитель: Соловьева М.В., к.ю.н., доцент

Саратовская государственная юридическая академия

СОВРЕМЕННЫЕ МЕТОДЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация: в данной работе рассматривается процесс расследования преступлений, совершенных с использованием информационных систем. Рассматриваются методы расследования подобных преступлений, в частности, киберфорензика. Кроме того, рассматриваются этапы киберфорензики. Также подробно описывается кибернетическая безопасность.

Ключевые слова: киберфорензика, компьютерные преступления, цифровые доказательства, киберпреступления, кибернетическая безопасность

V.V. Grigoriev

4th year student of the Institute of Law Enforcement

FGBOU VO "SGUA"

Saratov

Scientific supervisor: Solovieva M.V., Candidate of Law, Associate Professor

Saratov State Law Academy

MODERN METHODS OF INVESTIGATION

CRIMES COMMITTED USING INFORMATION SYSTEMS

Abstract: this paper examines the process of investigating crimes committed using information systems. The methods of investigation of such crimes, in particular, cyberforensis, are considered. In addition, the stages of cyberforensis are considered. Cyber security is also described in detail.

Keywords: cyberforensis, computer crimes, digital evidence, cybercrime, cybernetic security

Современные технологии и информационные системы стали неотъемлемой частью нашей жизни. Они упрощают и ускоряют многие процессы, но в то же время могут быть использованы для совершения преступлений. Глобальная компьютеризация играет значительную роль в технологическом оснащении преступности. В современном обществе информация закономерно перешла на новую ступень развития, стала товаром, получившим реальную стоимость, в связи с чем стала распространенным предметом посягательства. Сложность обнаружения действий компьютерного преступника и одновременно возможность без существенных усилий осуществлять криминальную активность делают данную категорию преступлений достаточно притягательной для злоумышленников и трудной в раскрытии для правоохранительных органов. Президент Владимир Путин, выступая на расширенной коллегии МВД, признал наличие проблем с раскрываемостью киберпреступлений. «За прошедший год увеличилось число раскрытых тяжких и особо тяжких. Но по другим направлениям динамика не столь позитивна. За последние шесть лет число преступлений в ИТ-сфере выросло в десять раз. Понятно, сами технологии быстро развиваются, мы за ними не успеваем», — заявил

президент в ходе выступления, которое транслировал телеканал «Россия 24»[1].

По данным Центрального Банка РФ ущерб от действий мошенников за 3 квартал 2022 года составил почти 4 миллиарда рублей, по инициативе банка было заблокировано около 300 тысяч мобильных номеров, 9 тысяч интернет сайтов, которые мошенники использовали для своих преступлений[2].

На первоначальных этапах расследования сотрудникам крайне важно уточнять у потерпевших все обстоятельства произошедшего, например, где и когда мошенники могли получить его персональные данные, на каких сайтах храниться или потерпевший сам предоставлял свои данные (к примеру, при покупке товаров онлайн на подозрительных источниках), о возможных потерях документов или их изменении, восстановлении. Всё это нужно для того, чтобы получить наиболее общую картину произошедшего, ведь, как правило, мошенники в сети интернет не работают в одиночку, поэтому подобная информация может помочь в выявлении всей схемы мошенников и привлечении их к ответственности.

Расследование такого рода преступлений должно осуществляться лицами, имеющими определенный набор навыков и знаний в сфере IT-технологий, с использованием инструментов разработанных и применяемых при расследовании данных преступлений. В этом и заключается специфика расследования данных деяний[3]. Поэтому, в целях улучшения общих показателей статистики преступных посягательств важно

---

[1] См.: Расширенное заседание коллегии МВД России от 3 марта 2021 года // URL: http://www.kremlin.ru/events/president/transcripts/65090 (дата обращения: 19 марта 2023 г.).

2 См.: Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // Официальный сайт Банка России (cbr.ru) URL: http://www.cbr.ru/analytics/ib/review_3q_2022/ (Дата обращения: 19 апреля 2023 г.).

3 См.: Карягина О.В. Система мер борьбы с мошенничеством / Достижения современной науки и образования. Кисловодск, 2017. С. 112.

обеспечить качественное, грамотное и профессиональное их расследование. На сегодняшний день в подготовке для сотрудников органов предварительного следствия применяются рекомендации и приемы, направленные на повышение эффективности их действий при раскрытии и расследовании подобных преступлений. Сейчас среди сотрудников применяются методы моделирования, компьютерного моделирования, анализ материалов уголовных дел предшествующих лет и т.п. Кроме того, помимо специалистов в области компьютерной техники, технологий и информации при расследовании уголовных дел рассматриваемой категории наиболее востребованы специалисты в сфере финансов, кредита и аудита, экономической безопасности, банковского дела, медицины и охраны труда.

Одним из главных методов расследования является киберфорензика. В сети интернет дано определение термина «киберфорензик» (англ. cyber forensics) обозначает он процесс сбора, анализа и интерпретации цифровых данных, которые могут быть использованы в качестве доказательств по делу. Данное определение недостаточно полно раскрывает этот термин. Н.Н. Федотов даёт свое определение понятия «киберфорензика», рассматривая его как компьютерную криминалистику, т.е. прикладную науку о раскрытии и расследовании преступлений в сфере компьютерной информации, связанную с исследованием следообразования цифровых доказательств, а также методов их выявления и различного рода технических средств, используемых в ходе совершения и расследования преступлений»[1]. Нельзя не согласиться с его мнением, ведь этот метод позволяет изучать цифровые следы, оставленные преступником в компьютерной системе. Киберфорензика включает в себя анализ жестких дисков, поиск удаленных файлов, изучение логов и другие методы. Киберфорензика может быть разделена на несколько основных этапов:

[1] См.: Федотов Н.Н. Форензика - компьютерная криминалистика М.: Юридический Мир, 2007. С.11.

1. Сбор данных - это первый этап киберфорензики, который включает в себя сбор и копирование цифровых данных с компьютеров, мобильных устройств, сетевых устройств и других электронных устройств.

2. Анализ данных - это этап, на котором эксперты киберфорензики используют специализированные инструменты и методы для анализа данных. Они ищут следы преступных действий, такие как удаление файлов, изменение данных или скрытие информации.

3. Интерпретация данных - на этом этапе эксперты киберфорензики используют свои знания и опыт для интерпретации полученных данных. Они могут выявить связи между различными элементами данных и определить, как они связаны с преступлением.

4. Представление данных - на последнем этапе киберфорензика эксперты представляют свои результаты в форме отчета, который может быть использован в юридических процедурах.

В результате эксперт может получить информацию о том, как преступник использовал компьютерную систему, какие данные он получил и как он их использовал.

Еще одним методом является мониторинг социальных сетей. С помощью специальных программ правоохранительные органы могут отслеживать активность преступников в социальных сетях и получать информацию о их планах и намерениях. Этот метод позволяет предотвратить совершение преступлений и задержать преступников на ранних стадиях.

Важно упомянуть о методе кибернетической безопасности. Этот метод включает в себя защиту информационных систем от хакеров и других злоумышленников. С помощью специальных программ и аппаратных средств можно обнаруживать и предотвращать попытки несанкционированного доступа к компьютерным системам. В целом, современные методы расследования преступлений с использованием

информационных систем позволяют правоохранительным органам более эффективно бороться с киберпреступностью и предотвращать совершение преступлений. Однако, необходимо помнить о необходимости соблюдения прав человека и конфиденциальности персональных данных при использовании этих методов.

Таким образом, киберфорензика является неотъемлемой частью современных методов расследования преступлений, связанных с использованием информационных систем. Поэтому очень важно развивать национальные методы противодействия, не забывая при этом обращаться к зарубежному опыту.

Также важным методом является использование программного обеспечения для анализа данных. Эти программы позволяют обрабатывать большие объемы информации, выявлять связи между преступниками и определять их местонахождение. Такой подход позволяет значительно ускорить процесс расследования и повысить его эффективность. Огромное значение имеет работа с носителями информации, ведь информация может быть зашифрована. Существуют тысячи инструментов расследования для каждого типа киберпреступности, доступных для выполнения криминалистической деятельности специалистами, например:

- Life Response;
- SIFT;
- TSK, The Sleuth Kit;
- X-Ways Криминалистика и другие.

Как отмечают А.А. Эксархопуло и В.Ю. Сокол в работе «Кризис отечественной криминалистики» российская криминалистика уже перестала быть дидактическим эталоном не только в странах, некогда строивших социализм, но и во многих государствах, отпочковавшихся от Советского Союза. Если российские криминалисты и дальше будут видеть свои научные интересы только лишь в национальных границах либо в

пределах русскоговорящих пространств, игнорируя, таким образом, свободный обмен научной информацией с коллегами из других стран мира, то наука, которую им выпала честь представлять, рискует рано или поздно остаться на обочине глобальных интеграционных процессов и превратиться в невостребованный конгломерат наукообразного типа» [1]. Но значительная часть российских ученых не согласна с такой позицией и считает, что никакого кризиса нет.

Нельзя отрицать, что большую роль в методах расследования подобных преступлений играют запросы в иностранные платежные ресурсы об предоставлении информации о переводах между счетами подозреваемых, но ответы на такие запросы делаются очень долго или не приходят вообще, что даёт преступникам возможность успешно отмывать украденные денежные средства и оставаться безнаказанными. Очень важно повышать качество и скорость взаимодействия органов и различных ресурсов (криптобиржы, киви и т.п.), а также совершенствовать национальное законодательство, ведь проблемы отсутствия контроля за криптовалютой позволяют мошенникам уходить от правосудия.

На основании изложенного можно сделать вывод о том, что в современных условиях существует большое количество методов расследования преступлений, совершенных с использованием информационных систем. С развитием общества, компьютерных технологий преступники становятся умнее и продумывают более изощренные способы совершения киберпреступлений. В этой связи одним из наиболее важных задач, стоящих перед сотрудниками правоохранительных органов, является совершенствование уже имеющихся методов расследования данной категории преступлений, а также внедрение

[1] См.: Эксархопуло А.А. Предмет и система криминалистики. Проблемы развития на рубеже XK — XX вв. Курс лекций. СПб., 2004. 112 с.; Сокол В.Ю. Кризис отечественной криминалистики. Краснодар, 2017. 332 с.

новых методов, отвечающих быстрому развитию и изменению способов совершения таких преступлений.

Использованные источники:

1. Берова Д.М. Расследование киберпреступлений // Пробелы в российском законодательстве. 2018. №1. С. 173-175.

2. Ваценко А.А. Обзор техник компьютерной криминалистики / Бюллетень науки и практики. 2020. С. 167-174.

3. Карягина О.В. Система мер борьбы с мошенничеством / Достижения современной науки и образования. Кисловодск, 2017. С. 111-113.

4. Сокол В.Ю. Кризис отечественной криминалистики. Краснодар, 2017. 332 с.

5. Федотов Н.Н. Форензика - компьютерная криминалистика. М.: Юридический Мир, 2007. 432 с.

6. Черных В.В. Проблемы расследования мошенничества, совершенного с использованием банковских карт, и пути их решения // Вестник Таганрогского института управления и экономики. 2018. №1. С. 123-126.

7. Эксархопуло А.А. Предмет и система криминалистики. Проблемы развития на рубеже XK — XX вв. Курс лекций. СПб., 2004. 112 с.

8. Расширенное заседание коллегии МВД России от 3 марта 2021 года // URL: http://www.kremlin.ru/events/president/transcripts/65090 (Дата обращения: 19 марта 2023 г.).

9. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // Официальный сайт Банка России (cbr.ru) URL: http://www.cbr.ru/analytics/ib/review_3q_2022/ (Дата обращения: 19 апреля 2023 г.).