СТАТЬЯ ПО ТЕМЕ «Особенности расследования преступлений

совершенных в сети интернет»

ARTICLE ON THE TOPIC " Features of the investigation of crimes committed on the Internet»

Гречинская В.И

 студент 4 курса

кафедры правоохранительной деятельности

и национальной безопасности

Южно – Уральский государственный университет

г. Челябинск

e-mail: VIKA.GRECHINSKAYA.98@mail.ru

Grechinskaya V. I

4rd year student

law enforcement departments

and national security

South Ural state University

g. Chelyabinsk

e-mail: VIKA.GRECHINSKAYA.98@mail.ru

**Аннотация:** В статье рассматриваются особенности расследования преступлений с сфере сети интернет.

**Abstract**: The article discusses the features of the investigation of crimes using the Internet.

**Ключевые слова**: расследование преступлений, интернет, информация, сеть.

**Keywords:** crime investigation, internet, information, network.

**Предмет:** Особенности расследования преступлений

совершенных в сети интернет

**Цель:** Рассмотреть особенности расследования преступлений в сети интернет

**Методология:** логический и статистический анализ

С развитием сети интернет и информационных технологий, компьютеризации и глобального внедрения техники в нашу жизнь, вплоть до полного перехода на электронный документооборот и совершение банковских операций онлайн и сеть все большую актуальность приобретают преступления в сфере компьютерной безопасности и сети интернет.

Эта разновидность преступлений отличается от большинства других тем, что в объективном мире остается мизерное количество следов, сама же объективная сторона преступления выражена в виртуальной реальности. К тому же, среднестатистический следователь, не обладающий специальными  знаниям в области сети интернет и информационных технологий, фактически не способен полноценно расследовать данный вид преступлений.

На сегодняшний момент в России пока еще нет такого всплеска преступлений в сфере сети интернет, как в странах Запада, но информатизация не стоит на месте, и буквально через 5-10 лет вопрос о необходимости подготовки следователей и дознавателей к расследованию данных деяний будет стоять очень остро.

Очевидно, что необходимо издание специальных инструкций, которые позволят эффективно разбираться в особенностях данного вида преступлений и дадут криминалистический анализ данных деяний, как это в свое время было сделано для других видов преступлений.

На сегодняшний момент такие преступления являются скорее нонсенсом, нежели рутинной работой правоохранительных органов.

Тем не менее, в криминалистической науке уже сегодня существуют, хотя и весьма скудные, основанные на опыте передовых стран сведения, позволяющие в общих чертах описать методику расследования данных преступлений.[[1]](#footnote-1)

Проблема заключается в том, что нет единого, комплексного исследования данного вопросов.

Итак, прежде чем приступить к изучению методики расследования преступлений в сфере сети интернет, следует изучить криминологические свойства самой информации в ней.

Во-первых, ее легко распространить путем копирования, передачи на расстояние, она быстро преобразуется из одного вида в другой.

Во-вторых, несмотря на то, что данная информация в интернете в объективной действительности не существует, она всегда привязана к физическому носителю, без которого она не сможет существовать.

Информация, в соответствии с законодательством, подразделяется на информацию общего пользования (общедоступную информацию) и информацию ограниченного доступа (конфиденциальную информацию). Последняя, как правило, и становится объектом преступных посягательств в силу своей значимости и ценности.[[2]](#footnote-2) В частности, к ней относятся все виды тайн, включая коммерческую тайну, и персональные данные в сети интернет.

В случае, если есть основания полагать, что имел место неправомерный доступ к информации в интернете, следует в первоочередном порядке выяснить следующие вопросы:

— был ли доступ действительно неправомерным;

— в какое время, из какого места, каким способом было совершено несанкционированное проникновение;

— каким способом оно было осуществлено;

— установления возможного круга лиц, предположительно совершивших или имеющих возможность совершить это преступление.

На базе знаний, полученных в ходе выяснения вышеназванных вопросов, у следователя должна сложиться вполне ясная картина преступления.

Круг субъектов, которые способны получить несанкционированный доступ к закрытым серверам или сетям компании, крайне ограничен в связи с тем, что преступник в данном случае должен обладать огромным багажом знаний в области информации в сети интернет и защиты ее.

Особенностями расследования преступлений в сети интернет следственная практика показывает, что чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно ограничен еще больше.

Понимание и прогнозирование поведения подозреваемого (обвиняемого) в интернет-мошенничестве имеют особую значимость в тактике допроса, который является процессуальной формой межличностного общения.

Представляется правильным согласиться с мнением некоторых исследователей, которые, в частности, указывают, что адаптация предварительного расследования к условиям реального приоритета личности представляет актуальную проблему криминалистики

Особенно такие приёмы должны быть востребованы при допросе подозреваемых и обвиняемых по делам о мошенничестве в сети Интернет, который обоснованно считается наиболее психологически сложным следственным действием. Сочетание данных особенностей обусловлено тем, что принципиально значимая информация о подготовке, совершении и сокрытии мошенничества находится в психике подозреваемого (обвиняемого), который часто является единственным обладателем этих сведений и зачастую активно противодействует их выявлению и процессуальному оформлению.[[3]](#footnote-3)

Поскольку подавляющее большинство интернет-мошенников лица, впервые совершившие преступление, то разумным при их допросе представляется применение рекомендаций по ведению допросов в отношении лиц, впервые совершивших мошенничество, однако с учетом их интеллектуального развития и специфических познаний в области современных информационных технологий.[[4]](#footnote-4)

 Поэтому при проведении следственных действий по данной категории преступлений необходимо учитывать следующие нюансы:

— заранее подготовится к изъятию носителя информации, на котором хранилась данная информация, в интернете т.к. он, как правило, содержит следы проникновения, изучение которых поможет достоверно установить способ и время, а возможно и место, из которого было совершено проникновение.

— прибыть на место как можно раньше, чтобы ограничить доступ всех лиц к данному устройству. Это связано с тем, что, как правило, именно сотрудники компании являются либо преступниками, либо соучастниками преступления, и могу попытаться скрыть следы преступления.

— отключить устройство от сети, дабы оградить его от повторного вмешательства через удаленное соединение.

— стараться до изъятия самостоятельно не проводить никаких манипуляций с техникой, если нельзя быть уверенным в результате того или иного действия.

Изъятие носителя должно быть произведено в соответствии с требованиями УПК РФ.[[5]](#footnote-5)

После того, как было изъято оборудование, подвергшееся несанкционированному доступу, следует обратить внимание на персонал компании, особенно на лиц, которые занимаются обслуживание ЭВМ, поддержанием сети и защитой информации. Основными подозреваемыми на первых этапах предварительного расследования являются те сотрудники, которые удовлетворяют следующим критериям:

— знали или могли знать о том, что на данном устройстве хранится информация, представляющая определенную ценность;

— обладают высоким навыком и специальными знаниями, позволяющими или предположительно дающими возможность совершения данного преступления;

Особого внимания заслуживают специалисты, которые занимаются защитой информации в сети от несанкционированного доступа, т.к. они, как правило, самостоятельно «пишут» программы, направленные на защиту информации и знают все их слабые и сильные стороны.[[6]](#footnote-6)

Помимо работающих в компании сотрудников, следует также обратить внимание на тех, кто работал в ней ранее и предположительно соответствовал тем критериям, которые были перечислены выше, как по трудовому договору, так и по гражданско-правовому.

Как правило, этих мер будет достаточно, чтобы раскрыть данное преступление. Тем не менее, иногда встречаются случаи, когда преступник обладает огромным опытом и новейшими технологиями, никогда не работал в данной компании, а сработал, например, по заказу или наводке. Таких хакеров в России единицы, но, тем не менее, они есть. Для раскрытия преступлений, совершенных ими, едва ли у правоохранительных органов хватит опыта и возможностей.

Как показывает статистика, раскрываемость компьютерных сетей преступлений в РФ достаточно низкая. Это связано с тем, правоохранительные органы встречается с этим видом преступлений крайне редко, и потому реального практического опыта и методики расследования данных видов преступлений ими пока не разработано.

Помимо этого, в большинстве компаний скупятся на покупку и использование современных программ и иных средств защиты информации в сети, что делает их уязвимыми для атак хакеров.

Скорее всего, ситуация с данными преступлениями в скором времени изменится. Наша страна, начиная с госорганов, уже активно внедряет электронный документооборот, электронные торги, онлайн заявки на оказания услуг. Все это влечет, с одной стороны, ускорение процессов подачи заявлений, а с другой — переносит их в менее защищенную реальность — виртуальную, где уже притаились охотники за данными, только и ожидающие момента, чтобы похитить слабозащищенную, но очень ценную информаци.

Использованная литература:

1. Уголовно-процессуальный кодекс Российской Федерации закон Российской Федерации от 18 12 2001 г № 174-ФЗ // Автоматизированная справочная правовая система «КонсультантПлтос»
2. Об информации, информационных технологиях и о защите информации закон Российской Федерации от 27 07 2006 г X» 149-ФЗ // Автоматизированная справочная правовая система «КонсульташПлюс».
3. Городов О. А. Комментарий к Федеральному закону «Об информации. информатизации и защите информации» / О. А. Городов СПб Нигер. 2003 224 с
4. Андреев Б. В. Расследование преступлений в сфере компьютерной информации / Б. В. Андреев, II Н. Пак, В II Хорст М Юрлигинформ. 2001 152 с
5. Крылов В. В. Информационные компьютерные преступления / В В Крылов М. НОРМА-ИНФРА-М. 1997 - 285
6. <https://www.bibliofond.ru/view.aspx?id=794950>
7. https://web.snauka.ru/issues/2017/08/84253
1. Развитие информационных технологий в уголовном судопроизводстве: монография / под ред. С.В. Зуева. - М. : Юрлитинформа, 2018. - 248 с. [↑](#footnote-ref-1)
2. Об информации, информационных технологиях и о защите информации закон Российской Федерации от 27 07 2006 г X» 149-ФЗ // Автоматизированная справочная правовая система «КонсульташПлюс». [↑](#footnote-ref-2)
3. . Крылов В. В. Информационные компьютерные преступления / В В Крылов М. НОРМА-ИНФРА-М. 1997 - 285 [↑](#footnote-ref-3)
4. Ефремов К.А. Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. - 2016. - № 6. - С. 92-95. [↑](#footnote-ref-4)
5. Уголовно-процессуальный кодекс Российской Федерации закон Российской Федерации от 18 12 2001 г № 174-ФЗ // Автоматизированная справочная правовая система «КонсультантПлтос»
 [↑](#footnote-ref-5)
6. Андреев Б. В. Расследование преступлений в сфере компьютерной информации / Б. В. Андреев, II Н. Пак, В II Хорст М Юрлигинформ. 2001 152 с [↑](#footnote-ref-6)