УДК 343.9

Рожнева Анастасия Александровна
Студент
1 курс, факультет «Юридический»
НОЧУВО МФПУ «Синергия»
Россия, г. Москва

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: *В данной статье раскрывается понятие компьютерной информации, нормативно-правовые акты регулирующие правоотношения в сфере компьютерной информации, а также характеристика преступлений в данной сфере. В конце статьи делается вывод о том, что процесс информатизации общества, особенно через его компьютеризацию приводит к увеличению количества компьютерных преступлений, их удельного веса в общей доле преступлений.*

Ключевые слова: *Компьютерная информация, криминалистическая характеристика преступлений, характеристика лица, совершающих преступления в сфере компьютерной информации, место совершения преступления, мотивы совершения, способ совершения преступления в сфере компьютерной информации.*

Annotation: *This article reveals the concept of computer information, regulatory legal acts regulating legal relations in the field of computer information, as well as the characteristics of crimes in this area. At the end of the article, it is concluded that the process of informatization of society, especially through its computerization, leads to an increase in the number of computer crimes, their specific weight in the total share of crimes.*

Key words: *Computer information, criminalistic characteristics of crimes, characteristics of the person committing crimes in the field of computer information, the place of commission of the crime, motives for committing, method of committing a crime in the field of computer information.*

Расследование преступлений в сфере компьютерной информации выступает одной из острейших задач современной криминалистической науки, это связано с проникновением компьютерных технологий во все сферы жизни человека.

К изучению компьютерных преступлений можно отнести таких ученых как, Н.П. Яблокова, Р.С. Белкина, В.А. Мещерякова и других.

В XX столетии появились такие средства коммуникации, как телефон, радио, телевидение, компьютер, позволяющие общаться не только непосредственно, но и на расстоянии, что значительно упростило жизнь современного человека.

С появлением компьютера жизнь людей во многом переменилась. Компьютерные технологии помогают оптимизировать работу в различных сферах деятельности человека. К тому же, появление компьютеров открыло новые возможности для досуга. Время не стояло на месте, и за считанные годы компьютерное производство превзошло все ожидания пользователей.

Проникновение компьютера во все сферы жизни деятельности человека, в значительной степени привело к компьютеризации информации, что значительно повлияло на доступность данной информации. На этой почве возникли предпосылки совершения преступлений данной категории.

Статья 23 Конституции РФ гласит о том, что «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» [1]. В данном случае будет нарушение конституционных прав человека.

Практика свидетельствует о том, что компьютерная техника все чаще выступает в качестве орудия совершения преступлений. В настоящее время ущерб, наносимый компьютерными преступлениями, сопоставим с доходами, получаемыми от внедрения современных компьютерных технологий. В 2021 году в России зарегистрировано около 518 тыс. киберпреступлений, что на 1,4% больше, чем годом ранее, но сразу в 1,8 раза превосходит показатель 2019 года. Об этом свидетельствуют данные компании RTM Group, которая проводила оценку на основе возбужденных уголовных дел, связанных с использованием информационных технологий. [2]

Проникновение компьютерных технологий в жизнь человека, не могло обойти стороной нашу страну. Первые компьютеры появились в России в конце 60-х годов. Последние годы компьютеризация российского человека достигла такого уровня, что возникла необходимость правового регулирования общественных отношений в этой сфере. Все это обуславливает разработку правовых норм, обеспечивающих регулирование общественных отношений, которые связаны с использованием и защитой компьютерной техники.

В связи с этим следует упомянуть Федеральный закон от 27 июля 2003 года «Об информации, информатизации и защите информации» [3]. До принятия в 1996 году Уголовного кодекса РФ [4], отечественное уголовное право не знало, а следственно никак не регулировало преступления в сфере компьютерной информации. Но после принятия нового УК появилась глава 28, посвященная преступлениям в сфере компьютерной информации, которая состоит из трех статей: "Неправомерный доступ к компьютерной информации" (ст. 272), "Создание, использование и распространение вредоносных программ для ЭВМ" (ст. 273), "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" (ст. 274), так же в связи с последними изменениями Уголовного Кодекса от 14.07.2017 года (Федеральный закон от 14.07.2022 N 260-ФЗ "О внесении изменений в Уголовный кодекс Российской

Федерации и Уголовно-процессуальный кодекс Российской Федерации"), появилась статья 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования», изменениями от 26.07.2017 года ("О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 194-ФЗ, появилась статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», а также изменениями от 29.11.2012 года (Федеральный закон от 29.11.2012 N 207-ФЗ (ред. от 03.07.2016) "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации"), появились статьи 159.3 «Мошенничество с использованием электронных средств платежа» и 159.6 «Мошенничество в сфере компьютерной информации». Наряду с этим в других главах УК предусмотрена ответственность за непредоставление информации (ст. 140 УК РФ); незаконный экспорт научно-технической информации (ст. 189 УК РФ); сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей (ст. 257 УК РФ), и за некоторые другие преступления, связанные с разглашением информации.

По нашему мнению, понятие «электронная вычислительная машина» устарело, т.к. компьютерные технологии стремительно развиваются, ведь почти каждый день выпускаются все новые и новые компьютерные технологии. Согласно ФЗ «Об информации, информатизации и защите информации», существует множество определений, характеризующих информационно-технологические средства, а самого понятия «компьютера»

нет. В связи с этим существует необходимость сформулировать новое понятие компьютерных технологий для того, чтобы законодатель не отдавал приоритет своих полномочий преступным группировкам.

Законодатель в ст. 2 ФЗ "Об информации, информатизации и защите информации" закрепляет, что «информация - сведения (сообщения, данные) независимо от формы их представления» [3].

В примечании к ст. 272 УК РФ дано определение компьютерной информации, под которой понимаются «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [4].

Предметом всей главы 28 Уголовного кодекса является носитель компьютерной информации, ЭВМ или компьютерные системы ЭВМ – совокупность компьютера и периферийного оборудования (принтер, сканер, факс). С объективной стороны преступления в сфере компьютерной информации совершаются в основном путем активных действий. Субъективная сторона выражается в форме умысла, как прямого, так косвенного. Субъектом данного вида преступлений будет лицо, достигшее 16 лет.

Необходимо отметить, что определение информационно-телекоммуникационных сетей закреплено в ст. 2 ФЗ "Об информации, информатизации и защите информации" – «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» [3].

Таким образом, преступления в сфере компьютерной информации представляют собой запрещенные уголовным законодательством, виновные посягательства на безопасность в сфере использования компьютерной информации, причинившие существенный вред или создавшие угрозу причинения такого вреда личности, обществу или государству.

Криминалистическая характеристика преступлений является самостоятельной отраслью в разделе криминалистики, определяющая значение, как в теоретической, так и в практической деятельности расследования преступлений данной категории дел.

Несмотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования данных преступлений, в этой области до сих пор остается ряд нерешенных и дискуссионных вопросов. Особенное место занимает криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации, «поскольку эти данные несут в себе важную криминалистически важную информацию, необходимую для определения направления расследования и поиска преступников. Особенно важны сведения об их профессиональных качествах, степени знания компьютерной техники, компьютерными программами и т.д.» [5]. Преступники, совершающие компьютерные преступления, как правило, характеризуются высоким интеллектуальным уровнем, наличием соответствующего опыта или специальной подготовки в области компьютерных средств, но также встречаются лица [5.С.305], так называемые «самоучки», то есть лица, не имеющие специальных знаний, а выучившиеся дома по книгам. (На жаргонном языке, так называемые «хакеры», «кракеры», «фрикеры»). Как правило, в случае совершения преступления в сфере компьютерной информации в отношении юридического лица, преступником или сообщником (пособником) является сотрудник данного учреждения, организации. Это − операторы ЭВМ, периферийных устройств и средств связи; программисты; системные администраторы; инженеры-электроники; администраторы баз данных; специалисты по сетевой безопасности, должностные и иные лица, имеющие доступ к компьютерной информации и оборудованию, их сети. [7]

Мотивы этого могут быть различными: хулиганские побуждения, озорство, месть, корыстные побуждения, промышленный и иной шпионаж и пр.

Место совершения преступления - это окружающие преступника обстановка, в которой осуществляется его преступная деятельность, характеризующая место, время, производственные, бытовые и другие условия и возможность совершения преступления.

Главная особенность места совершения компьютерных преступлений заключается в несовпадении между местом совершения противоправных действий и местом наступления общественно опасных последствий, то есть между местом, где преступление совершалось и местом наступления последствий этого деяния. Это характеризует преступления, совершенные при удаленном (опосредованном) доступе к компьютерной информации. Отсюда следует что, данные преступления могут носить межгосударственный характер, например само преступление, может быть совершено в России, а наступившие общественно опасные последствия в США.

Также существует такой способ совершения преступления как, непосредственный доступ к компьютерной информации или системе ЭВМ, при нем место совершения преступления и место наступления последствий может совпадать. Например, сотрудники банка, имеющие доступ ко всем данным, могут совершать противоправные действия прямо на рабочем месте. В этом случае место совершения противоправных действий и место наступления последствий этих действий совпадают.

Неправомерный доступ к компьютерной информации может производиться в зависимости от способа совершения преступления:

- в организациях, предприятиях при непосредственном доступе;
- в жилище, помещениях других предприятий или организаций, заранее арендованных помещениях, специально оборудованных автомобилях и т.п. при опосредованном доступе.

Распространение вредоносных программ может происходить в Интернете, в магазинах специализирующихся на продаже компьютерных программ и в иных местах.

Способов совершения компьютерных преступлений на данный момент существует великое множество, но далеко не все актуальны на данный момент – некоторые устарели, другие требует большого опыта от хакера, а другие просто не подходят для достижения цели хакера. Поэтому к выбору способа совершения преступления, злоумышленники подходят очень серьезно.

Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и, соответственно, определить наиболее оптимальные методы решения задач раскрытия преступления.

Выделяют следующие способы совершения компьютерных преступлений:

1. Похищение компьютерной техники;
2. Перехват информации;
3. Несанкционированный доступ к информации;
4. Манипуляция данными и управляющими командами;
5. Компьютерный саботаж;
6. Комплексные методы.

На сегодняшний день, существует широкий круг представлений о понятии криминалистической характеристике преступлений. Отсутствие, какого-то определенного понимания этой категории дает основания понять, что ученые до сих пор продолжают ее изучения. Потребности следственной практики, гласят о том, что, все элементы криминалистической

характеристики преступлений должны представлять собой научно обоснованные данные об обстоятельствах, типичных для преступлений конкретного вида или группы. Выделение элементов в структуре криминалистической характеристики должно быть вызвано потребностями практики и ею же оправдано.

Знание криминалистической характеристики личности как подозреваемого, так и потерпевшего во многом помогает облегчить деятельность следователя при раскрытии и расследовании преступлений в сфере компьютерной информации. Это важно, потому что не каждый может совершать преступления в данной сфере, для этого нужны специальные знания, они обладают отличительными чертами характерными только преступникам данного рода.

Информация об обстановке совершения преступления обычно является основой в криминалистической характеристике любого преступления, так как она во многом определяет и корректирует способ совершения преступления и в значительной мере сказывается на особенностях и структуре его механизма. В ней проявляются отдельные важные личностные черты преступника, формирующего (частично или полностью) данную обстановку, в большей или меньшей степени приспосабливающегося к ней или использующего ее без какого-либо приспособления, а иногда и без учета ее особенностей.

Обстановка, в которой совершаются компьютерные преступления, имеет главную отличительную черту, это не совпадение места совершения преступления и местом наступления общественно опасных последствий. Время совершения таких преступлений может быть разным, и оно зависит от способа совершения преступления.

Список литературы:

1. Конституция РФ от 12.12.1993.М.: Издательство ОМЕГА – Л, 2008.С – 62.

2. Число киберпреступлений в России: сайт TADVISER. [Электронный ресурс]. URL: https://www.tadviser.ru/a/593963.

3. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. N 149-ФЗ Режим доступа: СПС Консультант Плюс

4. Уголовный Кодекс РФ от 13 июня 1996 г. в ред. ред. от 14.07.2022, с изм. от 18.07.2022) (с изм. и доп., вступ. в силу с 25.07.2022) Режим доступа: СПС Консультант Плюс

5. Савельева М.В., Смушкин А.Б. Криминалистика. Учебник. – М.: "Деловой двор", 2009 г. С – 324.

6. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: Автореф. дис. Воронеж, 2001.

7. Клещёва, А.С. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации / А.С. Клещёва. — Текст: непосредственный // Молодой ученый. — 2018. — № 37 (223). — С. 57-60. — URL: https://moluch.ru/archive/223/52669/