**Чумакова Валерия Игоревна**
Студентка 1 курса юридического факультета,
Российский государственный социальный университет,
г. Москва, Российская Федерация

**Chumakova Valeriya Igorevna**
A student of the 1-st year of the law faculty,
Russian state social university,
Moscow, Russian Federation

# МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.
# Fraud in the field of computer information.

**Аннотация.**

Данная статья посвящена проблеме мошенничества в сфере компьютерной информации, а так же борьбе с ней.

**Ключевые слова:** мошенничество, безопасность, компьютерная информация.

**Abstract:.**

This article is devoted to the problem of fraud in the field of computer information, as well as the fight against it.

**Key words:** fraud, security, computer information.

Смена вектора развития современных государств от индустриального к информационному обществу стала причиной повсеместного внедрения высоких технологий практически во все сферы человеческой жизнедеятельности. Стремительная, практически неконтролируемая информатизация общества, при всех ее достоинствах, породила и ряд негативных явлений, одним из которых является криминализация телекоммуникационных и компьютерных систем связи. Рост числа компьютерных преступлений по всему миру обусловил принятие рядом зарубежных государств специального законодательства в этой сфере. Не стала исключением и Россия, включившая в Уголовный Кодекс главу 28,

посвященную преступлениям в сфере компьютерной информации. В условиях стремительной компьютеризации, захватившей практически все стороны жизни нашего общества, роста количества ЭВМ, используемых в России, недостаточного уровня защищенности компьютерной информации от противоправных посягательств, не исключено, что в скором времени проблема информационной безопасности станет в один ряд с такими глобальными проблемами современности, как экологический кризис, организованная преступность, коррупция, отсталость развивающихся стран и другие. Как показывают уголовная и судебная статистика, значительная часть таких преступлений остается за рамками реально выявленных и раскрытых.

Федеральным законом № 207-ФЗ от 29 ноября 2012 г. в действующий Уголовный кодекс Российской Федерации внесены изменения. Гл. 21 была дополнена шестью новыми составами, среди которых ст. 159.6 «Мошенничество в сфере компьютерной информации». Данная статья призвана защитить отношения собственности, имущественные интересы, отношения, обеспечивающие охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей. Уголовная ответственность предусмотрена за хищение чужого имущества или приобретение права на чужое имущество посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей . Совершение преступного деяния указанного в ст. 159.6 УК РФ возможно исключительно посредством использования современных компьютерных технологий. Компьютерная информация - это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. Особенность компьютерной информации заключается в следующем: она относительно просто пересылается, преобразовывается, размножается; при изъятии информации, в отличие от изъятия вещи, она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут одновременно иметь несколько пользователей.

Мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное законодательство. До настоящего времени основная деятельность в указанной сфере осуществлялась в рамках требований ст. 272-274 УК РФ. Прослеживается

схожесть объективной стороны деяний ст. 159.6 УК РФ и ч. 2 ст. 272 УК РФ, предусматривающей неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности. Однако если при мошенничестве ввод, удаление, блокирование, модификация либо иное вмешательство являются способами преступления, то, по смыслу диспозиции ст. 272 УК РФ, уничтожение, блокирование, модификация либо копирование информации выступают скорее обязательными последствиями. По моему мнению, предметом преступного посягательства по ст. 159.6 УК РФ являются:1) компьютерная информация, под которой в уголовно-правовом аспекте понимаются сведения (или сообщения, данные),представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, согласно положениям Примечания к ст. 272 УК РФ; 2) имущество, т. е. совокупность вещей, которые находятся в собственности лица, в т. ч. включая деньги и ценные бумаги, а также имущественных прав на получение вещей или имущественного удовлетворения от других лиц. Как мне представляется, в случае если лицо оперировало сведениями, не относящимися к компьютерной информации (в понимании уголовного закона), либо его действия не были связаны с завладением имуществом, а преследовали иные цели, (например, создание препятствий в реализации прав собственника), уголовная ответственность по ст. 159.6 УК РФ исключается. Скорее всего, уголовно-наказуемыми по ст. 159 УК РФ являются только лишь следующие общественно опасные способы завладения чужим имуществом:

ввод компьютерной информации, т. е. размещение сведений в устройствах ЭВМ для их последующей обработки и (или) хранения;

удаление компьютерной информации, т. е. совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации, и (или) в результате которых уничтожаются носители компьютерной информации;

блокирование компьютерной информации, т. е. совершение действий, приводящих к ограничению или закрытию доступа компьютерной информации, но не связанных с ее удалением;

модификация компьютерной информации, т. е. совершение любых изменений сведений (сообщений, данных), представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Под «вмешательством в функционирование» следует понимать осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного реального

обращения с компьютерной информацией. В современной следственно-судебной практике в Российской Федерации конструкция ст.159.6 УК РФ не всегда будет охватывать собой «традиционные» общественно опасные схемы хищения чужого имущества с использованием компьютерной техники и информации, а должна применяться к виновному лицу в совокупности с иными статьями УК РФ. Так, например, исходя из современной следственно судебной практики наиболее распространенным является деяние в виде хищения «электронных денег», состоящее из следующих «преступно логичных», последовательных «технических этапов»: ) неправомерное завладение компьютерной информацией (например, путем незаконного получения ключа доступа, логина, пароля и т. п.); ) использование похищенной компьютерной информации в целях дальнейшего присвоения чужого имущества.

Под «вмешательством в функционирование» следует понимать осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного реального обращения с компьютерной информацией. В современной следственно-судебной практике в Российской Федерации конструкция ст.159.6 УК РФ не всегда будет охватывать собой «традиционные» общественно опасные схемы хищения чужого имущества с использованием компьютерной техники и информации, а должна применяться к виновному лицу в совокупности с иными статьями УК РФ. Так, например, исходя из современной следственно судебной практики наиболее распространенным является деяние в виде хищения «электронных денег», состоящее из следующих «преступно логичных», последовательных «технических этапов»: ) неправомерное завладение компьютерной информацией (например, путем незаконного получения ключа доступа, логина, пароля и т. п.); ) использование похищенной компьютерной информации в целях дальнейшего присвоения чужого имущества.

Криминалистическая характеристика мошенничества в сфере компьютерной информации. Проанализируем отдельные элементы механизма мошенничества в сфере компьютерной информации с целью определения их взаимодействия между собой и влияния каждого из них на формирование криминалистических знаний о противоправном деянии. Прежде всего необходимы знания о компьютерных средствах. Как следообразующие объекты компьютерные средства выступают в двух аспектах: как носители информации о самом субъекте преступления . Особенность заключается в том, что компьютерные средства сами не являются следами преступной деятельности, так как не обладают

характерными специфическими особенностями, но при этом несут на себе следовую картину преступного деяния. Об этом свидетельствует анализ следственной практики, когда, например, при производстве следственных действий из компьютера изымается только его «жесткий диск» - запоминающее устройство для хранения информации. Между тем, технические характеристики компьютерно - технических средств и их наличие или отсутствие вообще должны свидетельствовать о возможности реализации преступного умысла (например, подключение или не подключение компьютера к телекоммуникационной сети). Большинство ученых сходятся во мнении, что основной характерной особенностью компьютерно - технических средств (с проекцией на потребности расследования) является их свойство сохранять информацию. С этим следует согласиться, потому что это и есть определяющий момент формирования криминалистического знания о компьютерных преступлениях и, в частности, такого вида, как мошенничество в сфере компьютерной информации.

Подводя итог вышеизложенному, хотелось бы сказать, что включение статьи о мошенничестве в сфере компьютерной информации в российское уголовное законодательство, с одной стороны, упростила процедуру выявления и расследования преступлений данной категории как на национальном, так и на международном уровне, исключила возможность уголовного преследования граждан Российской Федерации за совершение киберпреступлений на территории других стран и их ответственность по зарубежному уголовному законодательству. Мошенничество в сфере компьютерной информации является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное законодательство. До настоящего времени основная деятельность в указанной сфере осуществлялась в рамках требований ст. 272-274 УК РФ, формально подпадающих под положения Раздела «Offences against the confidentiality, integrity and availability of computer data and systems» (C.2, S.1, T1 Европейской Конвенции о киберпреступности ), фактически оставляя без внимания вопросы ответственности за совершение преступлений, связанных с использованием компьютерных средств («Computer-related offences»). Необходимость криминализации компьютерного мошенничества назрела давно, обоснованность принятия данной статьи раскрывается рядом научных статей, отражается в существующей практике. Фактически с включением ст. 159.6 УК РФ в национальное законодательство разрешен вопрос об участии Российской Федерации в мировых интеграционных процессах в сфере борьбы с

киберпреступностью, вектор которых определяется положениями Конвенции. Складывается ситуация, когда наша страна, формально не участвуя в Конвенции, тем не менее, развивает собственное национальное законодательство в соотнесении с существующей практикой борьбы с киберпреступностью.

## Список литературы


1. Конституция Российской Федерации от 12 декабря 1993 года (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ и от 30.12.2008 № 7-ФКЗ), п. 2 ст. 23.
2. Уголовный процесс: Учебник для вузов. / Под ред. А.В. Гриненко. М.: Норма, 2013.
3. Юшкевич А.В. Актуальные вопросы соблюдения тайны связи // Правовые вопросы связи. - 2008. - № 1. - С. 33-36.
4. Дунаева М.С. Проблемы защиты частной жизни граждан при осуществлении контроля и записи переговоров // Адвокатская практика. - 2003. - № 3.- С. 44-47.
5. Волынская О.В., Шишкин В.С. К вопросу о доказательственном значении сведений о телефонных соединениях // Российский следователь. - 2011. - № 2. - С. 12 - 15.
6. Смолькова И.В. Частная жизнь граждан: основания и пределы уголовно-процессуального вмешательства. - М., 1997.
7. Федеральный закон «О мошенничестве в сфере компьютерной информации» № 207-ФЗ от 29 ноября 2012 г..
8. Уголовно-исполнительное право: Учебник / Под ред. проф. И.В. Шмарова. М.: Изд-во Бек, 1998.
9. Уголовно-процессуальный кодекс Российской Федерации от 22 ноября 2001 года (в посл. ред. Федерального закона от 02.12.2008 № 226-ФЗ).
10. Лазарев В.В. Ограничение прав и свобод как теоретическая и практическая проблема // Журнал российского права. - 2009. - № 9.

11. Никодимов И.Ю АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ПРАВА. Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2016. № 1 (763). С. 147-160.
12. Новиков М.Ю., Никодимов И.Ю. ЮРИСПРУДЕНЦИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ В сборнике: УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ И НАКАЗАНИЕ.ОПЫТ РОССИИ И ЗАРУБЕЖНЫХ СТРАН. сборник статей по материалам научно-практической конференции. 2019. С. 160-166.
13. Сапожникова Е.С., Никодимов И.Ю. РОСТ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ В сборнике: Правовое и криминалистическое обеспечение судебного исследования преступлений. Сборник статей по материалам Общероссийской конференции, посвященной памяти проф. В.В. Колкутина. Под редакцией В.Ю. Голубовского. 2019. С. 120-124.
14. Никодимов И.Ю. НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДМЕТА ИНФОРМАЦИОННОГО ПРАВА Правовое поле современной экономики. 2015. № 12. С. 135-140.
15. Гоголь А.А., Никодимов И.Ю. СТРАНИЦЫ ИСТОРИИ РАДИОСВЯЗИ (КОНЕЦ XIX – ПЕРВАЯ ЧЕТВЕРТЬ XX В.) Санкт-Петербург, 1998.