

Министерство образования и науки Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра уголовного,  
экологического права  
и криминологии

**Уголовно-правовая характеристика преступления  
мошенничество в сфере компьютерной информации  
(ст. 159.6 УК РФ)**

**АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ**

студента 4 курса 433 группы  
направления 40.03.01 «Юриспруденция»  
юридического факультета  
Солдатенко Александра Сергеевича

Научный руководитель  
д.ю.н., профессор

Н.Т. Разгельдеев

Зав. кафедрой уголовного,  
экологического права  
и криминологии  
докт. юрид. наук, профессор

Н.Т. Разгельдеев

Саратов 2017

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования** состоит в том, что в условиях глобальной компьютеризации, захватившей практически все стороны жизни нашего общества, роста количества ЭВМ, используемых в России, недостаточного уровня защищенности компьютерной информации - стремительно развиваются новые направления преступной деятельности, связанной с применением новейших технологий.

Бесспорно, технологический прогресс является положительным явлением для всего человечества - внедрение большого количества ЭВМ способствует улучшению условий существования человечества, делает жизнь более комфортной, однако так же создает возможности для развития новых направлений преступной деятельности. Одним из таких преступных деяний, потребовавших внесения изменений в действующее уголовное законодательство, стало мошенничество в сфере компьютерной информации. Случаи мошенничества, в основе которых лежит использование разнообразной экономически значимой компьютерной информации, в настоящее время получают все большее распространение.

С 10 декабря 2012 года в Уголовный кодекс внесены поправки согласно которым законодатель выделил шесть новых видов мошенничества<sup>1</sup>. Среди преступлений против собственности особое место занимает мошенничество в сфере компьютерной информации. Мошенничество в сфере компьютерной информации, согласно пункту 1 статьи 159.6 Уголовного Кодекса Российской Федерации - есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Отсутствие четкого определения компьютерной преступности,

---

<sup>1</sup> "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 17.04.2017)

единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

Всё вышеизложенное подтверждает актуальность темы преступлений в сфере компьютерной информации, необходимость и своевременность её комплексного и глубокого исследования.

**Целью данной дипломной работы является:** комплексное исследование объективных и субъективных признаков мошенничества в сфере компьютерной информации, рассмотрение квалифицирующих признаков данного деяния, а также выявление и анализ отличий преступления мошенничества в сфере компьютерной информации от других форм посягательства на собственность и смежных составов преступлений.

Исходя из данной цели были выдвинуты и решались следующие **задачи**:

1. Дать понятие, характеристику и провести уголовно-правовой анализ состава преступления мошенничество в сфере компьютерной информации как форм хищения чужого имущества.

2. Рассмотреть объективные признаки мошенничества в сфере компьютерной информации в соответствии со ст.159.6 УК РФ

3. Произвести разграничения мошенничества в сфере компьютерной информации от других форм хищений и смежных составов преступлений.

4. Сформировать макет уголовного дела с доказательной базой верной квалификации при использовании криминалистических методов и приемов в соответствии с уголовно-процессуальным законодательством.

5. Сделать свои предложения по совершенствованию профилактической деятельности правоохранительных органов, повышения эффективности и уменьшения количества преступлений против собственности, расследования преступлений в экономической сфере.

**Объект исследования дипломной работы** являются общественные отношения, подвергающиеся посягательствам в результате совершения преступлений в сфере компьютерной информации.

**Предмет исследования** являются уголовно-правовые нормы, устанавливающие ответственность за мошенничество в сфере компьютерной информации, практика их применения.

Нормативной базой исследования явились положения закрепленные в Конституции Российской Федерации, уголовном, уголовно процессуальном и другом федеральном законодательстве нашей страны постановлениях Конституционного Суда Российской Федерации, а также Пленума Верховного Суда РФ, ведомственных подзаконных актах (приказах указаниях, распоряжениях, инструкциях правоохранительных органов страны).

**Новизна исследования**, проведенного в дипломном исследовании, обусловлена как актуальностью выбранной темы, так и практическими задачами, стоящими перед правоприменителем. В исследовании сделан целый ряд предложений и заключений ранее в данной форме в исследованиях не фигурирующих, направленных на совершенствование мер уголовно-правовой борьбы с мошенничеством в сфере компьютерной информации.

**Информационной базой** исследования, обеспечивающей достоверность выводов, явились данные монографических, учебных изданий и периодической печати, законодательные и нормативные акты РФ, регулирующие отношения в области ответственности за мошенничество в сфере компьютерной информации.

**Методологическая основа** работы определялась характером предмета, целью и задачами исследования. В работе применялись методы системного и сравнительного анализа, качественной и количественной оценки рассматриваемых явлений, а так же методы теоретического исследования такие как, анализ и синтез.

В соответствии с целями и задачами данной работы структура ее состоит из введения, трех глав, заключения и списка использованной литературы.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Глава 1 «Уголовно-правовая характеристика мошенничества в сфере компьютерной информации» включает три параграфа.

Параграф 1.1 раскрывает общую характеристику состава преступления, предусмотренного ст. 159.6 УК РФ

Параграф 1.2 раскрывает объективные признаки преступления мошенничество в сфере компьютерной информации.

Параграф 1.3 раскрывает Субъективные признаки преступления мошенничество в сфере компьютерной информации

Глава 2 «Особенности квалификации и проблемы совершенствования уголовных норм мошенничества в сфере компьютерной информации» состоит из двух параграфов.

Параграф 2.1 раскрывает некоторые спорные вопросы квалификации мошенничества в сфере компьютерной информации.

Параграф 2 раскрывает содержание некоторых предложенных мер совершенствования уголовно-правовой борьбы мошенничества в сфере компьютерной информации.

Глава 3 «Макет уголовного дела (ст. 159.6 УК РФ)» содержит макет уголовного дела преступления, предусмотренного ст.159.6 УК РФ – мошенничество в сфере компьютерной информации.

Федеральным законом № 207-ФЗ от 29.11.2012 в действующий Уголовный кодекс Российской Федерации включена статья 159.6 «Мошенничество в сфере компьютерной информации», которая предусматривает ответственность за преступное посягательство на собственность и право собственности с использованием компьютерных технологий<sup>2</sup>.

Мошенничеством в сфере компьютерной информации, согласно ст.159.6 УК РФ, является хищение чужого имущества или приобретение

---

<sup>2</sup> Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" от 29.11.2012 N 207-ФЗ

права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Мошенничество в сфере компьютерной информации является квалифицированным видом преступления, предусмотренным статьей 159 УК РФ - мошенничество.

Объективную сторону мошенничества в сфере компьютерной информации составляет действия направленные на хищение чужого имущества, равно приобретения права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей и повлекшее указанные в ст. 159.6 УК РФ последствия. Данное преступное деяние возможно совершить исключительно путем использования современных компьютерных технологий.

Объект преступления предусмотренного ст. 159.6 УК РФ общественные отношения, складывающиеся по поводу имущества и юридически выраженного права владения, пользования и распоряжения этим имуществом собственником, в которое так же входит обязанность других лиц воспринимать указанные правомочия как должное и не препятствовать их осуществлению.

Совершение данного вида преступления, с точки зрения субъективной стороны, предполагает наличие вины в форме прямого умысла, когда виновное лицо осознает общественную опасность своих действий, предвидит реальную возможность или неизбежность наступления общественно опасных последствий (интеллектуальный момент) и желает их наступления (волевой момент). Таким образом мошенник должен полностью осознавать, что путем ввода, удаления, блокирования модификации либо иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной

информации, он завладевает чужим имуществом или правами на него. О наличии такого умысла может свидетельствовать сам факт заведомо-отсутствующего у виновного лица права на вторжение в информационные базы имущества потенциальных жертв. Данное обстоятельство не обязательно свидетельствует о наличии факта совершения преступления мошенничества в сфере компьютерных информации, в каждом конкретном случае должно быть достоверно установлено, что лицо, совершившее определенные в диспозиции статьи 159.6 УК РФ действия, заведомо намеревалось использовать полученную информацию в корыстных целях. Такие действия в зависимости от обстоятельств дела могут содержать признаки приготовления или покушения на совершение данного вида преступления.

Субъект преступления – лицо достигшее 16 летнего возраста.

Введение новой статьи в УК РФ является закономерным шагом интеграции российского законодательства о борьбе с компьютерными преступлениями в международное законодательство. Таким образом складывается ситуация, когда Российская Федерация формально не участвует в Конвенции, однако развивает собственное национальное законодательство в соответствии с существующей практикой борьбы с компьютерными преступлениями. Результатом включения законодателем в состав Уголовного Кодекса РФ новой статьи является конкретизация компьютерных преступлений, выделение среди них преступлений, совершаемых с использованием компьютерных средств, что в свою очередь так же порождает ряд проблем.

В диспозиции ст. 159.6 УК РФ мошенничество в сфере компьютерной информации определяется, как хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-

телекоммуникационных сетей. Таким образом, формулировка указанного состава преступления, принятая российским законодательством совпадает с дефиницией, предложенной Европейской Конвенцией о киберпреступности, которая в ст. 8 под мошенничеством с использованием компьютерных технологий понимает «лишение другого лица его собственности путем любого ввода, изменения, удаления или блокирования компьютерных данных, либо вмешательства в функционирование компьютерной системы, с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица».

Квалифицированный вид преступления по ст. 159.6 УК РФ имеет место в случае совершения деяния:

- деяния, совершенного группой лиц по предварительному сговору (ч.2);
- с причинением значительного ущерба гражданину (ч.2);
- совершения лицом с использованием своего служебного положения (ч.3);
- совершения в крупном размере (ч.3);
- совершения организованной группой (ч.4);
- совершения в особо крупном размере (ч.4).

Преступление, предусмотренное ч. 1 ст. 159.6 УК РФ является преступлением небольшой степени тяжести, преступления, предусмотренные ч. 2 и 3 ст. 159.6 УК РФ, — преступлениями средней тяжести, а преступления, предусмотренные ч. 4 указанной статьи, — отнесены к тяжким.

**В заключении** подведены итоги бакалаврской работы, представлены основные результаты и предложения по совершенствованию мер уголовно-правовой борьбы с преступлением «мошенничество в сфере компьютерной информации».

**Выводы:** Объективными признаками преступления, предусмотренного ст. 159.6 УК РФ являются – объект, которым в данном случае, является складывающиеся по поводу имущества и юридически выраженного права владения, пользования и распоряжения этим имуществом

собственником, дополнительным объектом по ч. 1 ст. 159.6 УК РФ является компьютерная информация. Объективная сторона мошенничества в сфере компьютерной информации выражается деянием в форме действия, направленного на хищение собственности путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, последствием в виде материального ущерба и причинной связью между ними.

Субъективная сторона преступления, предусмотренного ч. 1 ст. 159.6 УК, характеризуется как прямым умыслом. Субъект преступления – лицо достигшее 16 летнего возраста.

#### **Предложения:**

Современная ситуация в Российской Федерации в сфере борьбы с различными формами мошенничества требует принятия комплекса мер в нескольких направлениях: в развитии концепции борьбы с преступлениями в экономической сфере, отвечающих требованиям современной ситуации в стране; в совершенствовании организационно-структурного обеспечения борьбы с мошенничеством с учетом накопленного в течение последних 10 лет опыта расследования преступлений данного вида; в разработке комплекса высокоэффективных мер борьбы, подлежащих включению в федеральную и региональные целевые программы по усилению борьбы с преступностью; в совершенствовании уголовно-правового, административно-правового, гражданского-правового нормативного обеспечения мер борьбы с мошенничеством, с учетом реальной современной социально-экономической ситуации; в развитии информационно-методического обеспечения деятельности по предупреждению, в расследовании и назначении наказаний за мошенничество; в разработке комплекса мер, обеспечивающих достаточный контроль за лицами, ранее совершавшими мошенничество, а так

же в совершенствовании мер в отношении обеспечения возмещения вреда, причиненного мошенническими посягательствами.

Совокупность различных экономических, политических, психологических, технических, правовых, организационных и иных факторов способствует совершению и развитию новых способов, методов и схем данного вида преступления, что в свою очередь обуславливает актуальность проблемы борьбы России с мошенническими преступлениями разного рода, в том числе и мошенничеством в сфере компьютерной информации.

Среди множества различных мер предупреждения данного вида преступления можно выделить несколько основных групп – общесоциальные, организационные, технические и правовые.

К числу общесоциальных мер предупреждения преступления можно отнести следующие: общее укрепление экономики страны, повышение эффективности работы государственных органов, обеспечивающих нормальное функционирование российской экономики, улучшение системы защиты имущественных прав государства, субъектов экономической деятельности и граждан, обеспечение государственных гарантий защиты прав граждан, пострадавших в результате мошеннических действий. К организационным мерам стоит отнести: обеспечение заблаговременного выявления фактов мошенничества, в экономической сфере, организацию эффективного расследования и привлечения к уголовной ответственности лиц, совершивших мошеннические посягательства, организацию исполнения гражданско-правовых исков, позволяющих возместить причиненный ущерб потерпевшим от мошеннических преступлений, обеспечение содействия со стороны государственных органов жертвам мошенничества, службам безопасности организаций, в целях предупреждения, выявления, расследования и раскрытия мошеннических посягательств.

Исходя из того, что данный вид преступления связан с обязательным использованием компьютерной информации при совершении

противоправного посягательства, то необходимо так же применять меры совершенствования, направленные на обеспечение достаточной безопасности такой информации.

Говоря об организационно-технических мерах борьбы с преступлениями в данной сфере, можно выделить опыт зарубежных стран, который показывает, что одним из наиболее действенных способах защиты от компьютерных преступлений является введение в штатное расписание организаций должности специалиста по компьютерной безопасности, либо создание специальных как частных, так и государственных служб, основная деятельность которых будет заключаться в обеспечении безопасности в компьютерно-информационной сфере. Наличие таких служб, по оценкам специалистов, снижает вероятность совершения преступлений вдвое. Так же к организационно-техническим мерам борьбы с компьютерными преступлениями, в том числе и мошенничества в сфере компьютерной информации, можно отнести следующие мероприятия: создание информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации; организация подготовки и повышения квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров и учебных курсов, что позволит сотрудникам МВД России осуществлять расследование мошенничества в сфере компьютерной информации с достаточными навыками и знаниями; обеспечение государственных органов необходимыми технологическими ресурсами; разработка и осуществление скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере компьютерной информации, а так же обмен информацией о готовящихся или совершенных преступлениях в сфере компьютерной информации и причастных к ним физических и юридических лицах; о способах совершения преступлений в сфере компьютерной информации; о формах и методах

предупреждения, выявления, пресечения, раскрытия и расследования преступлений в данной сфере между государственными органами Российской Федерации. Так же можно выделить следующие возможные способы совершенствования мер борьбы с преступлениями в сфере компьютерной информацией: создание программ, регистрирующих первичные данные, которые исключают возможность пропуска обязательных реквизитов данных и содержат условия блокирования ввода-вывода информации и подсказку о пропущенных реквизитах; идентификация регистрирующейся личности при вводе первичных данных (то есть при авторизации данных), основанное на идентификации личности, производящей ввод-вывод данных, и предусматривающее возможность блокировки средств компьютерной техники при выполнении предъявляемых условий идентификации; создание различных программ защиты зарегистрированных данных от преднамеренного или случайного их искажения, уничтожения и от несанкционированного получения сведений о зарегистрированных данных. А так же создание условий и программ, которые позволяют исправлять машинную запись первичных данных только тем лицам, имеющим специальные полномочия, а основным подтверждением достоверности записи при этом - однозначная идентификация личности, производившей регистрацию первичных данных.

К другой группе мер предупреждения мошеннических посягательств являются правовые меры. К основным направлениям совершенствования уголовно-правовой борьбы с мошенничеством можно отнести следующие: совершенствование отдельных институтов Общей части УК РФ в целях дополнительной их ориентации на обеспечение борьбы с мошенничеством и прежде всего его организованными формами; восполнение дефицита уголовно-правовой охраны экономических отношений, вызванного недостатками законодательства, а также появлением новых форм мошенничества; снижение уровня неопределенности диспозиций и санкций норм об ответственности за мошенничество; определение суровости

наказания за отдельные виды мошенничества в соответствии с их общественной опасностью; совершенствование норм об ответственности за профессиональную мошенническую деятельность; совершенствование системы норм об ответственности за мошенничество, связанной с использованием компьютерной техники, компьютерных сетей и технологий.

Профилактика любого вида преступления, в том числе и компьютерного, должна носить комплексный характер и относиться к компетенции государственных органов, а не различных коммерческих охранных структур. Таким образом, реализация таких организационно – управленческих, технологических, общесоциальных и правовых мер и мероприятий в полном или частичном объеме, на наш взгляд, сильно повлияет на реальную ситуацию по профилактике, предупреждению, расследованию и раскрытию органами государственной власти преступлений в сфере и в связи с использованием компьютерной информации в Российской Федерации.