**ОМСКАЯ АКАДЕМИЯ МВД РОССИЙСКОЙ ФЕДЕРАЦИИ**

вариант №6

Тема:

Компьютерное мошенничество, вызванное манипуляциями программами ввода\вывода и платежными средствами (QFM, QFP)

Выполнил:

слушатель 4 курса

ФЗОиПК

Омской Академии МВД РФ

лейтенант милиции

Вышегородцев А.Н.

**ОМСК - 2005**

**П Л А Н**

Введение 3

Понятие компьютерного мошенничества 5

Особенности методики расследования 7

Доказательства по делам о преступлениях в сфере компьютерной информации, проблемы получения и использования 12

Заключение 15

Список использованной литературы 15

# Введение

Научно-технический прогресс постепенно приводит современное общество к тотальной компьютеризации наиболее важных областей общественной жизни. Наличие компьютерной информации потенциально связано с ее утечкой, разрушением, риском противоправного изъятия либо дополнением необъективной информацией. Автоматизация процессов обработки информации, отсутствие ее надлежащей защиты, повсеместное применение персональных электронно-вычислительных машин и некоторые другие объективные факторы делают ее уязвимой для преступных манипуляций

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран. [[1]](#footnote-1)

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы **Q**. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

1. **QA** - Несанкционированный доступ и перехват
2. **QAH** - компьютерный абордаж
3. **QAI** - перехват
4. **QAT** - кража времени
5. **QAZ** - прочие виды несанкционированного доступа и перехвата
6. **QD** - Изменение компьютерных данных
7. **QUL** - логическая бомба
8. **QDT** - троянский конь
9. **QDV** - компьютерный вирус
10. **QDW** - компьютерный червь
11. **QDZ** - прочие виды изменения данных
12. **QF** - Компьютерное мошенничество
13. **QFC** - мошенничество с банкоматами
14. **QFF** - компьютерная подделка
15. **QFG** - мошенничество с игровыми автоматами
16. **QFM** - манипуляции с программами ввода-вывода
17. **QFP** - мошенничества с платежными средствами
18. **QFT** - телефонное мошенничество
19. **QFZ** - прочие компьютерные мошенничества
20. **QR** - Незаконное копирование
21. **QRG** - компьютерные игры
22. **QRS** - прочее программное обеспечение
23. **QRT** - топография полупроводниковых изделий
24. **QRZ** - прочее незаконное копирование
25. **QS** - Компьютерный саботаж
26. **QSH** - с аппаратным обеспечением
27. **QSS** - с программным обеспечением
28. **QSZ** - прочие виды саботажа
29. **QZ** - Прочие компьютерные преступления
30. **QZB** - с использованием компьютерных досок объявлений
31. **QZE** - хищение информации, составляющей коммерческую тайну
32. **QZS** - передача информации конфиденциального характера
33. **QZZ** - прочие компьютерные преступления

Целью данной работы является изучение характера и особенностей преступлений связанных с *манипуляциями программам ввода\вывода(QFM)* и в сфере электронных *платежных средств(QFP),* ответственность за совершенные преступления.

# Понятие компьютерного мошенничества

Согласно международному классификатору, исследуемые мошенничества классифицируются как:

* **QFM** - манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается метод Подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ;
* **QFP** - компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

В Уголовном законодательстве России пока нет специального состава, предусматривающего ответственность за компьютерное мошенничество, тогда как, в уголовном законодательстве ряда зарубежных стран (таких как ФРГ, США, Эстония, Беларусь) предусмотрена уголовная ответственность за данное преступление.

В современной науке пока не выработано понятие компьютерного мошенничества. Очень мало исследований, посвященных данной проблеме. Так, одни авторы под компьютерным мошенничеством понимает корыстное преступное посягательство, в ходе выполнения которого осуществляются манипуляции с программами, данными или аппаратной частью ЭВМ. Другие считают, что компьютерное мошенничество – это компьютерное преступление, включающее умышленное искажение, изменение или раскрытие данных с целью получения выгоды (обычно в денежной форме) с помощью компьютерной системы, которая используется для совершения или прикрытия одиночного или серийного преступления. Компьютерная система может использоваться при неправомерном манипулировании исходными данными, входящими результатами, прикладными программами, файлами данных, работой компьютера, связью, оборудованием, системным программным или аппаратно-программным обеспечением

В настоящее время к компьютерному мошенничеству относятся преступные деяния, которые могут квалифицироваться по статьям о мошенничестве (ст. 159 УК РФ), о присвоении или растрате (ст. 160 УК РФ), о причинении имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ), об изготовлении или сбыте поддельных кредитных либо расчетных карт и иных платежных документов (ст.187 УК РФ).

До принятия нормы, предусматривающей ответственность за компьютерное мошенничество, рассматриваемое понятие следует считать криминологическим.

Итак, под компьютерным мошенничеством мы понимаются завладение чужим имуществом путем обмана, злоупотребления доверием, присвоения, растраты, а также причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенные с использованием средств компьютерной техники.

Предметом компьютерного мошенничества будет выступать имущество. Следует иметь ввиду, что предметом компьютерного мошенничества, как и преступлений против собственности, может быть только чужое имущество.

Объективная сторона компьютерного мошенничества может состоять в завладении чужим имуществом или правом на него, либо в причинении имущественного ущерба путем обмана или путем злоупотребления доверием, включая присвоение вверенного имущества с использованием средств компьютерной техники.

Обман при компьютерном мошенничестве выражается в завладении чужим имуществом либо правом на него, либо в причинении иного имущественного вреда путем умышленного искажения или сокрытия данных, вводимых в автоматизированную систему (преступление типа QFM), с целью введения в заблуждение лица, либо в манипуляциях с программами, данными или аппаратной частью ЭВМ, обрабатывающими информацию о передвижении имущества, с тем, чтобы добиться получения чужого имущества, права на имущество, либо получения иной имущественной выгоды.

Совершение хищения путем кражи с использованием средств компьютерной техники невозможно потому, что кража является тайным хищением чужого имущества. В компьютере не хранятся денежные средства или имущество, в компьютере хранится информация об этом имуществе или передвижении данного имущества. Если преступник тайно проникает в компьютерную систему с целью похитить денежные средства либо имущество, то он проникает в систему путем манипуляций с программами, данными либо техническими средствами (QFP). Как было сказано ранее, эти действия будут являться обманом, который специфичен для компьютерного мошенничества. Если происходит тайное копирование (кража) чужой информации, для неправомерного обладания ею, то данное деяние должно квалифицироваться по ст.272 – неправомерный доступ к компьютерной информации, повлекшее за собой уничтожение, блокирование, модификацию либо копирование информации.

#

# Особенности методики расследования

Методика расследования рассматриваемых преступлений характеризуется следующими особенностями:

- организация следственной деятельности при получении первичной информации;

- типизация следственных ситуаций;

- определение круга обстоятельств, подлежащих доказыванию;

- разработка программ расследования;

- организация предупредительной деятельности следователей;

- тактика следственных и иных действий.

По источникам возникновения первичная информация делится на две части:

1) возникшая в результате совершенного преступления, имеющего признаки преступной деятельности организованной преступной группы в сфере компьютерных технологий;

2) свидетельствующая о криминальном образе жизни лица или группы лиц; их прежней преступной деятельности; о связях в преступной среде; причастности к созданию, хранению, сбыту программного обеспечения; проявляемых антиобщественных намерениях; наличии теневых денежных сумм.

Наиболее важными факторами, влияющими на характер следственных ситуаций первоначального этапа расследования, являются:

- направление, или «ветвь», преступной деятельности;

- содержание преступных действий;

- характер информации о событии преступления;

- последствия преступления;

-результаты предшествующей работы по проверке первичной информации;

-данные, подтверждающие совершение преступления организованной криминальной группой, задействовавшей компьютерные системы.

Перечисленные факторы и их сочетания образуют следующие наиболее типичные для первоначального этапа расследования преступлений следственные ситуации:

1. Идет активная подготовка членов организованной преступной группы с приобретением компьютерной техники, программного обеспечения, вовлечением специалистов к совершению преступления.

2. Происходит осуществление членами преступной группы длящегося преступного деяния, связанного со взломом защиты компьютерной информации.

3. Имеется факт уже законченного тяжкого преступления, совершенного криминальной группой с использованием информационных технологий.

Гипотетические представления, применительно к судебно-следственной деятельности именуемые версиями, не могут возникать беспочвенно. Базой для их формирования являются обстоятельства реальной жизни, те или иные факторы, относящиеся к событию преступления. Многообразие и сложность криминальных ситуаций создает обстановку для решения многочисленных мыслительных задач, подавляющее число которых носит не алгоритмический, а творческий характер.

Фрагментарный характер большинства ситуаций выражается в отдельных следах, свидетельских показаниях, тех или иных вещественных доказательствах. В то же время, комплекс сведений, относящихся к событию преступления, нередко осложнен инсценированием обстановки преступления, фальсификацией следов, созданием ложной информации, не позволяющими придти к правильным выводам и предположениям путем анализа имеющейся информации. Разрыв естественных, закономерных причинно-следственных связей нередко направляет расследование по ложному пути, ведет к утрате доказательственной информации. Все названное свидетельствует о сложной мыслительной деятельности следователя, прокурора, судьи, связанной с расследованием преступления и судебным разбирательством. Если в этом отношении обратиться к условному делению (классификации) мыслительных задач, разрешаемых в процессе расследования, в их огромном числе, различном по уровню сложности, можно определить следующие:

1) задачи по обнаружению доказательственной информации;

2) задачи по оценке доказательств и оперативной информации;

3) задачи по выдвижению версий различной направленности;

4) задачи по принятию юридически значимых решений.

Все перечисленные задачи связаны между собой событием преступления и имеют своей целью его раскрытие. В этом плане мыслительные задачи можно разделить на группы: 1) задачи-алгоритмы, где ход решения типичен и заранее известен, определен нормой закона или процессуальной процедурой; 2) задачи эвристические, творческие, возникающие в связи с проблемной ситуацией и не имеющие заранее данного хода решения.

Значительная часть мыслительных задач, относящихся к расследованию компьютерных преступлений, совершенных организованными преступными группами и хакерами одиночками, являются творческими, т.е. требующими поиска таких путей решения, которые выходят за пределы элементарных рассуждений. Не всегда поставленные задачи могут быть разрешены на основании только имеющейся исходной информации.

Мыслительный анализ множества факторов приводит к формированию версий – обоснованному предположению в отношении преступного события в целом или отдельных его частей. Обращение к классификации каких-либо объектов, свойств, ситуаций способствует более четкому определению их видов и выполняемых функций. Классификации в различных областях знаний имеют не только теоретическое значение – выяснение характеристик различного рода объектов, но и практическое, позволяющее более конкретно определить назначение каждого класса, его роль в осуществлении практической деятельности. Проблемы классификации имеют место в отдельных разделах криминалистической тактики, а именно там, где существует определенное множество следственных действий, тактических приемов, рекомендаций, направленных на оптимизацию следственной деятельности.

При расследовании преступлений в сфере компьютерных технологий, возможна выработка ряда специфических версий, в теории которых были предприняты попытки классификации. Одни из авторов предпочитали такое дробление версий, при котором они могли относиться как к событию в целом, так и к отдельным его обстоятельствам, то есть, по существу разделяли их на общие и частные версии. Так, А.Н. Васильев отмечал, что версия – это предположение о наличии преступления в исследуемом событии, его характере, элементах состава преступления, отдельных обстоятельствах и их значении, а также о виновных лицах, формах вины, мотивах и целях преступления .[[2]](#footnote-2)

Как видно из определения, градация версий достаточно подробная, позволяющая распределять их относительно тех пунктов определения, которые указаны. Однако, другие авторы не разделяли столь широкой градации, указывая, что следственная версия – это предположение относительно «основных, наиболее существенных обстоятельств, которые в совокупности образуют то, что в уголовном праве носит наименование – состав преступления»[[3]](#footnote-3).

Заслуживает внимания высказывание Р.С. Белкина о том, что уровень версии объясняется совокупностью исходных данных, а границы совокупности определяются уровнем построенных на этих исходных данных предположений. Генеральная совокупность, определяющая значительное число данных, будет относиться к генеральной версии, меньшая совокупность – к уровню частных версий. Таким образом, первым классификационным основанием является совокупность исходных данных, или объем понятий. По этому основанию версии разделяются на общие и частные. Наряду с названным, основанием для классификации версий являются субъекты выдвижения версий. К ним относятся лица, которые по своим служебным функциям связаны с расследованием преступлений. В этой связи версии разделяются на розыскные, следственные, экспертные, судебные. По степени определенности версии следует делить на типичные и конкретные.[[4]](#footnote-4)

По своей сути версии являются ретроспективными, поскольку направлены на познание преступного события, имевшего место в прошлом. Однако, установление преступника, предполагаемого места его нахождения, миграции, последующих преступных действий (подготовка, совершение и сокрытие) – суть перспективной версии.

Таким образом, анализ элементов криминалистической характеристики преступлений в сфере информационных технологий позволяет сделать вывод о приоритете перспективных следственных и оперативных версий прогностического характера, касающихся преступлений такого рода («типового очага»); сферы посягательства (финансовые биржи, отраслевые информационные системы); мотивированной направленности посягательства (политические, экономические, хулиганские); уровня подготовки и тенденций к совершенствованию «преступного мастерства»; уровня организованности, динамики преступной, интеллектуальной, территориальной и по сферам. Учет основных прогностических характеристик данного вида преступлений может играть заметную роль при выработке стратегии расследования компьютерных преступлений и в ходе оперативно-розыскной деятельности.

# Доказательства по делам о преступлениях в сфере компьютерной информации, проблемы получения и использования

Получение и анализ доказательств по делам о преступлениях в сфере компьютерной информации (компьютерных преступлений) - одна из основных и трудно решаемых на практике задач. Ее решение требует не только особой тактики производства следственных и организационных мероприятий, но и прежде всего наличия специальных знаний в области компьютерной техники и программного обеспечения.

При расследовании компьютерных преступлений следователь сталкивается с необходимостью выявления и изъятия следов и собирания доказательств на следующих объектах исследования - компьютерной системе, телекоммуникационной сети или носителе информации (магнитном, оптическом и т.п.). При этом в некоторых случаях приходится искать нечто неосязаемое, а не привычные физические улики в виде следов применения оружия, отпечатков пальцев, поддельных документов и т.п. Объектами поиска могут быть даже записи в виде электронных импульсов в запоминающих устройствах работающего компьютера или телекоммуникационной сети.

Основные проблемы связаны с описанием подлежащего изъятию компьютерного оборудования и компьютерной информации, а также с тактикой проведения обыска. (Своеобразие тактических приемов и технических средств, применяемых для поиска, обнаружения, фиксации и изъятия доказательственной информации, хранящейся в компьютерной системе, позволяет, по нашему мнению, говорить об обязательном участии в производстве таких следственных действий, как осмотр, обыск и выемка компьютерных систем, специалистов в области компьютерных технологий. Особые сложности при производстве следственных действий по делам рассматриваемой категории характерны для распределенных компьютерных систем обработки информации. В этом случае место совершения преступления часто не совпадает с местом происшествия и наступления преступного результата.

Корректное получение и использование имеющейся доказательственной информации требует наряду со знанием юридических норм наличия как специальных технических устройств, так и специальных знаний из области информационных систем и информационных технологий. Поэтому при проведении расследований по делам о компьютерных преступлениях необходимо привлечение специалистов экспертной службы, имеющих полный набор технического обеспечения и уникального служебного программного обеспечения для организации успешного расследования, и назначение особого рода экспертиз, которые получили название компьютерно-технических .

Изучение специальной литературы на предмет проведенных компьютерно-технических экспертиз и анализ имеющихся результатов позволяет сделать определенные выводы по кругу задач, которые могут быть успешно решены с их помощью.

В отношении носителей информации:

прочтение и распечатка данных с машинных носителей информации;

восстановление данных на машинном носителе, подвергшихся удалению или модификации;

расшифровывание закодированных данных.

В отношении компьютерных систем:

установление обстоятельств (даты, времени) помещения данных на машинный носитель и возможных действий с ними (модификации, удаления, копирования и т.д.);

вскрытие систем защиты (пароли, электронные ключи)

выявление программно-аппаратных средств для несанкционированного доступа к машинным данным (модификации, копирования, блокирования и уничтожения данных);

установление места совершения преступления;

установление каналов доступа к защищаемой информации и путей ее возможной утечки;

установление технических параметров оборудования, его состояния, возможностей аппаратно-программной модификации и т.д.

В отношении лиц, эксплуатирующих компьютерную систему: установление авторства данных, средств и способов их подготовки на машинных носителях (файлов документов, вредоносных программ и т.д.);

установление уровня квалификации проходящих по делу лиц в области технических средств и программного обеспечения (компьютерных технологий).

Приведенный список задач не претендует на полный охват, однако отражает очевидные особенности рассматриваемых экспертиз: комплексный характер и потребность в привлечении специальных познаний. Эти особенности служат, по нашему мнению, достаточным основанием для выделения уже в настоящее время самостоятельного класса судебных экспертиз, которые можно назвать судебной экспертизой компьютерных (информационных) систем.

Уже сегодня многие традиционные преступления, такие как мошенничество, подделка ценных бумаг, заведомо ложная реклама, пропаганда насилия, распространение порнографических материалов совершаются с использованием современных информационных технологий, в частности, глобальной сети Интернет. Выделение особого класса судебных экспертиз, который охватывал бы практически все основные задачи по делам, связанным с использованием компьютерных технологий, должно способствовать построению целостной доказательной базы и эффективному решению поставленных экспертных задач.

# Заключение

В ходе проделанной работы были рассмотрены и изучены некоторые разновидности компьютерных преступлений связанных с мошенничеством, методика проведения расследования преступлений в данной сфере, особенности и проблемы сбора доказательств преступления, ряд необходимых экспертиз. Также рассмотрена законодательная база для данного вида преступлений.

# Список использованной литературы

1. Ахтырская Н.Н. Организованная преступность в сфере информационных технологий © Центр исследования проблем компьютерной преступности http://www.crime-research.org/library/Aht\_tem4.htm
2. Белкин Р.С. Курс криминалистики. - Т.3.С.372.
3. Васильев А.Н. Основы следственной тактики. М., 1960.С.15
4. Згадзай О.Э., Казанцев С.Я**.** Доказательства по делам о преступлениях в сфере компьютерной информации: проблемы получения и использования. © Центр исследования проблем компьютерной преступности http://www.crime-research.org/library/Zgaday.htm
5. Классификация компьютерных преступлений Генерального Секретариата Интерпола - http://makcim.yaroslavl.ru/crime.htm
6. Справочно-правовая система (СПС) «ГАРАНТ-СТУДЕНТ» (cd-осень2002)
7. Теребилов В.И. К вопросу о следственных версиях и планировании расследования // Сов. криминалистика на службе следствия. М., 1955. - Вып. 6.
8. Шаталов А.С., Пархоменко А.Н. Криминалистическая характеристика компьютерных преступлений © Центр исследования проблем компью-терной преступности http://www.crime-research.org/library/Shatal.htm
1. Классификация компьютерных преступлений - http://makcim.yaroslavl.ru/crime.htm [↑](#footnote-ref-1)
2. Васильев А.Н. Основы следственной тактики. М., 1960.С.15 [↑](#footnote-ref-2)
3. Теребилов В.И. К вопросу о следственных версиях и планировании расследования // Сов. криминалистика на службе следствия. М., 1955. - Вып. 6. - С.109. [↑](#footnote-ref-3)
4. Белкин Р.С. Курс криминалистики. - Т.3.С.372. [↑](#footnote-ref-4)