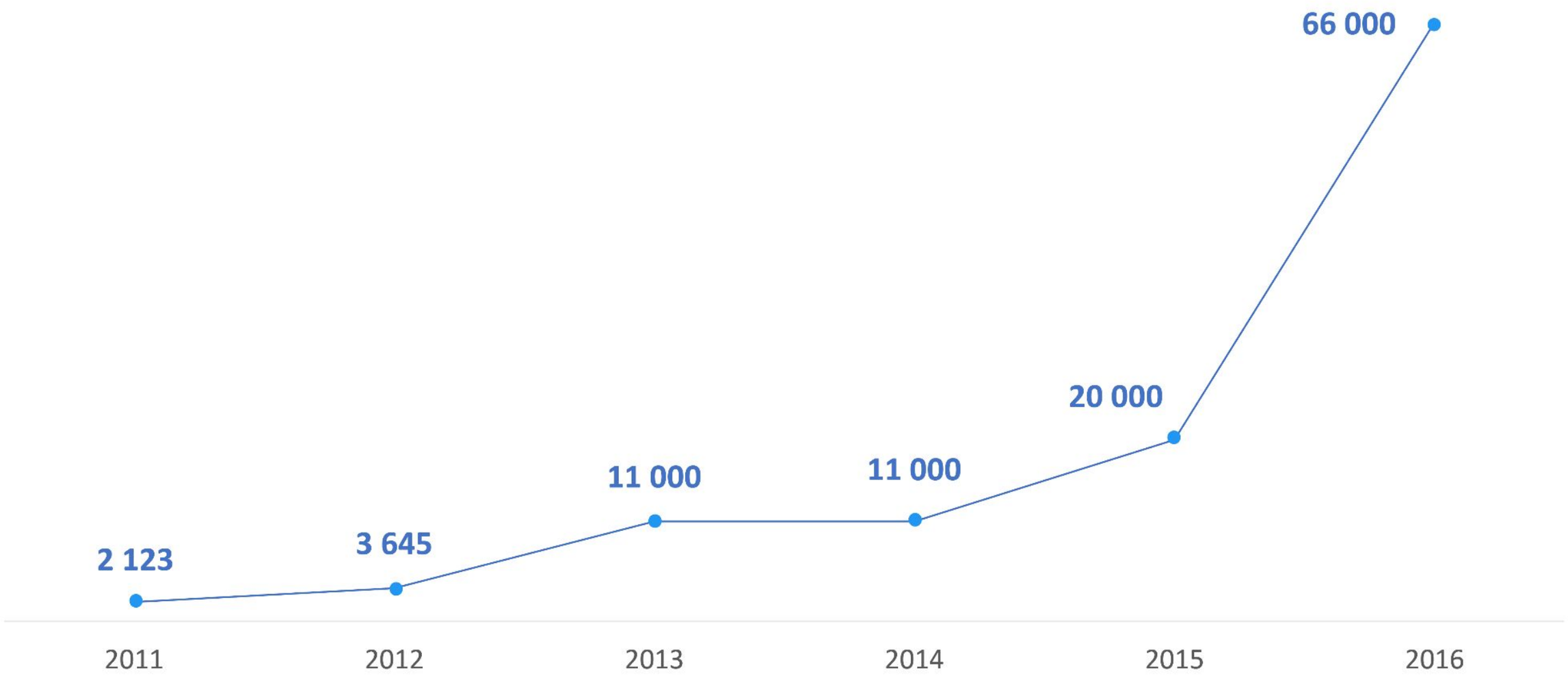
# КОМПЬЮТЕРНОЕ МОШЕННИЧЕСТВО

# Первое компьютерное преступление в СССР было зарегистрировано в **1979 г.** в Вильнюсе Ущерб 80 тыс.руб.

# Первый обвинительный приговор по компьютерному преступлению в России был **19.01.1997 г.**

# Преступления с использованием компьютерных и телекоммуникационных технологий




по данным Генеральной прокуратуры и МВД РФ

# Топ-3 наиболее острых проблем

1. Неумышленные действия или некомпетентные действия, приводящие к порче, сбою в работе оборудования, носителей информации.

2. Использование нелегальных программ, неизвестного происхождения, приводящих к временной или необратимой порче оборудования или программного обеспечения.

3. Разглашение, передача, утрата ключей, паролей, программ, приводящих к угрозе их несанкционированного использования.

# Технологии совершения компьютерного мошенничества:

1. Эквайринг (доступ к POS-терминалу);
2. С помощью NFC – считывателя;
3. Социальная инженерия;
4. С помощью своего человека в банке;
5. Внедрение вирусов;
6. Через социальные сети.

# Технологии совершения компьютерного мошенничества

**Эква́йринг** — приём к оплате платежных карт в качестве средства оплаты товара, работ, услуг. Осуществляется уполномоченным банком-эквайрером путём установки на торговых или сервисных предприятиях платёжных терминалов.

# Технологии совершения компьютерного мошенничества

**Социальная инженерия - метод получения информации.**

**Фишинг** – получение доступа к конфиденциальным данным пользователей (логинам, паролям).

**Популярные фишинговые схемы** – несуществующие ссылки, использование брендов известных корпораций, подложные лотереи, ложные антивирусы, телефонный фишинг, плечевой серфинг.

# Ст. 159.6 Мошенничество в сфере компьютерной информации

2012 год

В ст. 159.6 УК РФ предусмотрена ответственность за мошенничество в сфере компьютерной информации.

**Диспозиция** ст. 159.6 УК РФ - 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.

# Ст. 159.6 Мошенничество в сфере компьютерной информации

Данный вид мошенничества, на сегодняшний день, вызывает самое большое количество вопросов, связанных с пониманием признаков, описанных в диспозиции компьютерного мошенничества, что приводит к неправильной уголовно-правовой квалификации содеянного.

## Примечание к ст. 158 УК РФ

Под хищением понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

# Соотношение ст. 159 УК РФ и ст. 159.6 УК РФ

**СТ. 159 УК РФ**

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием

**СТ. 159.6 УК РФ**

Мошенничество в сфере компьютерной информации, то 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

# Соотношение ст. 159 УК РФ и ст. 159.6 УК РФ

**СТ. 159 УК РФ**

Наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.

**СТ. 159.6 УК РФ**

Наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

# Объект и предмет преступления по ст. 159.6 УК РФ

**Объект преступления**

- Собственность;
- Безопасность в сфере компьютерной информации;

**Предмет преступления**

- Чужое имущество или право на имущество;
- Компьютерная информация,

поскольку виновные воздействуя на нее, получают доступ к чужому имуществу.

# Кодекс Российской Федерации об административных правонарушениях

## Статья 7.27. Мелкое хищение

**Мелкое хищение чужого имущества путем** кражи, **мошенничества**, присвоения или растраты **при отсутствии признаков преступлений, предусмотренных** частями второй, третьей и четвертой статьи 158, частями **второй, третьей и четвертой** статьи 159, частями второй, третьей и четвертой статьи 159.1, частями второй, третьей и четвертой статьи 159.2, частями второй, третьей и четвертой статьи 159.3, частями второй и третьей статьи 159.4, частями второй, третьей и четвертой статьи 159.5, **частями второй, третьей и четвертой статьи 159.6** и частями второй и третьей статьи 160 Уголовного кодекса Российской Федерации.

# Уголовный кодекс Российской Федерации
# Статья 159 Мошенничество

5. Мошенничество, сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, если это деяние повлекло причинение значительного ущерба;

6. Деяние, предусмотренное частью пятой настоящей статьи, совершенное в крупном размере;

7. Деяние, предусмотренное частью пятой настоящей статьи, совершенное в особо крупном размере.

**Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»**

Не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты, если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать по соответствующей части статьи 158 УК РФ.

# Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»

Хищение чужих денежных средств, находящихся на счетах в банках, путем использования похищенной или поддельной кредитной либо расчетной карты следует квалифицировать как мошенничество только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации (например, в случаях, когда, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя).

## Уголовный кодекс Российской Федерации

### Статья 159.3 Мошенничество с использованием платежных карт

1. Мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации

# Имущество и право на имущество как предмет компьютерного мошенничества

Имущество всегда может быть предметом.

- Вещи;
- Наличные и безналичные денежные средства;
- Ценные бумаги (документарные и бездокументарные).

Вопрос о том, может ли право на имущество быть предметом, остается открытым.

- Права требования;
- Исключительные права.

(Постановление Пленума Верховного Суда РФ от 17.12.2015 N 56 «О судебной практике по делам о вымогательстве»)

# Из Постановления Пленума ВС РФ от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве»

К предмету вымогательства по смыслу статьи 163 УК РФ относится, в частности, **чужое** (то есть не принадлежащее виновному на праве собственности) **имущество**, а именно **вещи**, включая **наличные денежные средства**, документарные **ценные бумаги**; **безналичные денежные средства**, **бездокументарные ценные бумаги**, а также **имущественные права**, в том числе **права требования и исключительные права**.

## Из Постановления Пленума ВС РФ от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве»

Под **правом на имущество**, с передачей которого могут быть связаны требования при вымогательстве, в статье 163 УК РФ понимается **удостоверенная в документах возможность осуществлять правомочия собственника или законного владельца в отношении определенного имущества**.

# Документарные ценные бумаги

Ценными бумагами являются документы, соответствующие установленным законом требованиям и удостоверяющие обязательственные и иные права, осуществление или передача которых возможны только при предъявлении таких документов.

# Бездокументарные ценные бумаги

Ценными бумагами признаются также обязательственные и иные права, которые закреплены в решении о выпуске или ином акте лица, выпустившего ценные бумаги в соответствии с требованиями закона, и осуществление и передача которых возможны только с соблюдением правил учета этих прав в соответствии со ст. 149 ГК РФ.

В том случае, когда имеет место противоправное приобретение права на бездокументарные ценные бумаги, указанное право, согласно Федеральному закону от 22 апреля 1996 г. N 39-ФЗ "О рынке ценных бумаг", удостоверяется в системе ведения реестра - записями на лицевых счетах у держателя реестра (регистратора) или в случае учета прав на ценные бумаги в депозитарии - записями по счетам депо в депозитариях. Поэтому внешняя форма закрепления права на имущество может проявляться как в бумажной, так и в электронной форме.

Анализ судебной практики показывает, что право на имущество рассматривается как право собственности на недвижимое имущество, право на долю в уставном капитале, право требования денежных средств  и т.д.

В качестве разновидностей имущества как предмета мошенничества в сфере компьютерной информации чаще всего выступают денежные средства в безналичной форме. В отдельных уголовных делах фигурирует иное имущество, имеющее овеществленную форму.

Так, С. был заключен договор возмездного оказания услуг с ООО "Р", согласно которому С. обязалась совершать действия, направленные на увеличение объема продаж торговой марки "А". В качестве покупателя в базе клиентов ООО "Р" была зарегистрирована Е. Имея умысел на хищение чужого имущества путем модификации компьютерной информации, С. модифицировала личные данные на странице Е., получив доступ к личной странице Е.

После чего С. оформила от имени Е. интернет-заказ на доставку товара марки "А" и экспресс-доставку на свое имя. Таким образом, С. путем модификации компьютерной информации похитила товар компании "А". Сложно, однако, согласиться с признанием именно товара предметом преступления, поскольку путем модификации компьютерной информации С. изъяла денежные средства, находящиеся на счете Е., и распорядилась ими по своему усмотрению путем заказа товара марки "А"

# Статья 1226 ГК.РФ Интеллектуальные права

**Исключительное право** — совокупность принадлежащих правообладателю (гражданину или юридическому лицу) прав на использование по своему усмотрению любым не противоречащим закону способом результата интеллектуальной деятельности или средства индивидуализации и на запрещение или разрешение такого использования другими лицами.

# Статья 1226 ГК.РФ Интеллектуальные права

Дело №1-638/11.

Иванькова В.Н., совершившего преступления, предусмотренные ст.146 ч.2 УК РФ, ст.273 ч.1 УК РФ.

Иваньков В.Н., не имея прав на использование, в том числе и распространение объектов авторского права, вопреки воле правообладателей и в нарушение ч.1 ст. 44 Конституции РФ и ст. ст.1225, 1229, 1259, 1261, 1262, 1280 и других статей глав 69-71 части 4 Гражданского Кодекса РФ, решил незаконно использовать объекты авторского права с целью извлечения прибыли и причинения ущерба в крупном размере, путем распространения контрафактного программного обеспечения:, «***», правообладателем которых является корпорация «***», контрафактного программного обеспечения, правообладателем которого является корпорация «***», контрафактного программного обеспечения «***», правообладателем которого является корпорация «***».

## Статья 1226 ГК.РФ Интеллектуальные права

Дело №1-638/11.

Иваньков В.Н., реализуя умысел на незаконное использование объектов авторского права с целью извлечения прибыли и причинения материального ущерба в крупном размере вопреки воле правообладателя, находясь в квартире по предварительной договоренности с покупателем об оплате и комплектности программного обеспечения, с имевшихся при себе *** оптических дисков с контрафактным программным продуктом и флеш-накопителя, установил на накопитель на жестких магнитных дисках «***», находящихся внутри системного блока персонального компьютера, не разрешенные правообладателями «***», «***» и «***» к свободному распространению программные продукты.

## Статья 1226 ГК.РФ Интеллектуальные права

Дело №1-638/11.

После этого Иваньков В.Н. продемонстрировал покупателю работоспособность установленных им программных продуктов, получив в указанной квартире в качестве оплаты от покупателя деньги в сумме *** рублей, после чего сразу же был задержан сотрудниками милиции. Иваньков В.Н., незаконно используя объекты авторского права в крупном размере, распространил контрафактные экземпляры

# Что такое информационная безопасность?

В уголовном законодательстве нет определения понятия «информационная безопасность».

Настоящее понятие дается в Постановлении Правления ПФ РФ от 26.01.2001 N 15:

«О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи» (вместе с «Регламентом регистрации и подключения юридических и физических лиц к системе электронного документооборота Пенсионного фонда Российской Федерации»).

# Что такое информационная безопасность?

Информационная безопасность (безопасность информации) - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

# Компьютерная информация как предмет компьютерного мошенничества

Компьютерная информация, с помощью которой виновный осуществляет обманные действия и завладевает имуществом, является дополнительным предметом компьютерного мошенничества. Однако, то, с помощью чего совершается преступление, именуется в уголовном праве средством, а не предметом.

«Справка-обобщение изучения судебной практики рассмотрения судами Самарской области уголовных дел о преступлениях, предусмотренных ст. ст. 159.1-159.6 УК РФ, отграничение от смежных составов. Практика назначения наказания»

# Что такое компьютерная информация?

Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Примечание к ст.. 272 УК РФ.

Компьютерная информация - информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи.

Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации.

# Что такое компьютерная информация?

**СОВЕТ ЕВРОПЫ**

Конвенция о преступности в сфере компьютерной информации (ETS N 185)

(Будапешт, 23 ноября 2001 года)

Компьютерные данные означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию.

# Термин «компьютерная информация»

- Представляется, что понятие «компьютерная информация» следует заменить на «электронная информация», так как компьютерная информация является одним из ее видов.

- Имеет значение, что ввиду недостаточной ясности термина «электрический сигнал», используемый для раскрытия понятия «компьютерной информации», представляется необходимым изъять его из законодательного определения.

Под электронной информацией можно было бы понимать ***сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи***».

# Где может содержаться компьютерная информация?

В настоящее время компьютерная информация может содержаться в устройствах, которые внешне не напоминают компьютер:

- Планшетные компьютеры; Мобильные телефоны; Банкоматы; Платежные терминалы; и др.

Поэтому логичнее было бы говорить о компьютерных системах.

Компьютерная система – любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных. *(Конвенция о преступности в сфере компьютерной информации)*

# Способы компьютерного мошенничества

Мошенничество в сфере компьютерной информации должно характеризоваться двумя способами:

ст. 159 УК РФ

Обман

**или**

Злоупотребление доверием.

+

ст. 159.6 УК РФ

Ввод, удаление, блокирование, модификация компьютерной информации

**или**

Иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Не всегда способом компьютерного мошенничества выступает обман или злоупотребление доверием конкретного лица, так как путем воздействия на компьютерную информацию вводится в заблуждение компьютерная система (которая не является физическим лицом).

# Способы компьютерного мошенничества

## Обман

Обман как способ совершения хищения или приобретения права на чужое имущество, ответственность за которое предусмотрена статьей 159 УК РФ, может состоять в сознательном сообщении заведомо ложных, не соответствующих действительности сведений либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение.

# Способы компьютерного мошенничества

## Обман

Сообщаемые при мошенничестве ложные сведения (либо сведения, о которых умалчивается) могут относиться к любым обстоятельствам, в частности к юридическим фактам и событиям, качеству, стоимости имущества, личности виновного, его полномочиям, намерениям.

# Способы компьютерного мошенничества

## Злоупотребление доверием

Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо личными или родственными отношениями лица с потерпевши

# Способы компьютерного мошенничества

Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»

## Злоупотребление доверием

Злоупотребление доверием также имеет место в случаях принятия на себя лицом обязательств при заведомом отсутствии у него намерения их выполнить с целью безвозмездного обращения в свою пользу или в пользу третьих лиц чужого имущества или приобретения права на него (например, получение физическим лицом кредита, аванса за выполнение работ, услуг, предоплаты за поставку товара, если оно не намеревалось возвращать долг или иным образом исполнять свои обязательства).

**«Ввод»** → **«Доступ»**

Ввод компьютерной информации – это взаимодействие двух и более объектов компьютерной информации (один из которых является «агрессором») без изменения структуры программного кода атакуемого объекта.

Доступ к компьютерной информации – возможность получения информации и ее использование (ФЗ №149-ФЗ «Об информации, информационных технологиях и о защите информации»).

## Ввод информации

Анализ практики вменения такого признака, как "ввод информации", показывает, что правоприменительные органы чаще всего признают ввод самостоятельным способом в том случае, когда виновные, осознавая факт подключения к его СИМ-карте чужой банковской карты, формируют СМС-сообщение, отправляют его на номер "900", в результате чего производят перечисление денежных средств. Например, Г., используя сотовый телефон с СИМ-картой оператора сотовой связи ОАО "Мегафон", зарегистрированной на его имя, обнаружив, что к данному абонентскому номеру СИМ-карты с помощью услуги "Мобильный банк" ОАО "Сбербанка России" подключена международная банковская карта ОАО "Сбербанка России", принадлежащая А., на лицевом счете которой находятся денежные средства, решил совершить хищение.

## Ввод информации

С этой целью Г., действуя умышленно, из корыстных побуждений, совершая мошенничество в сфере компьютерной информации, путем ввода компьютерной информации сформировал СМС-сообщение в виде электрических сигналов для перевода денежных средств. Данное СМС-сообщение Г. направил на номер "900", указав в тексте сообщений суммы подлежащих перечислению денежных средств. Таким образом, Г. осуществил перевод со счета международной банковской карты ОАО "Сбербанка России" на счет своего абонентского номера СИМ-карты денежных средств, получив возможность распоряжаться похищенными денежными средствами по своему усмотрению .

В представленном примере применение такого способа, как "ввод информации", признано единственным признаком компьютерного мошенничества, поскольку суд посчитал, что действия по набору информации не привели к последствиям в виде ее блокирования, уничтожения, модификации.

Еще одно дело № 1-1296/2016

**«Ввод»** → **«Доступ»**

Доступ к информации - понятие более широкое и в большей мере отражает то воздействие на информацию, которое необходимо при совершении компьютерного мошенничества.

Как показывает судебная практика совершение хищение чужого имущества путем доступа к компьютерной информации возможно без ее модификации, удаления, блокирования.

# Последствия ввода/доступа

Неправомерный доступ к компьютерной информации - это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации. При этом под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее).

"Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации"
(утв. Генпрокуратурой России)

# Блокирование информации

Блокирование информации - результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением.

"Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации"
(утв. Генпрокуратурой России)

# Модификация информации

Модификация информации - внесение изменений в компьютерную информацию (или ее параметры). Законом установлены случаи легальной модификации программ (баз данных) лицами, правомерно владеющими этой информацией, а именно: модификация в виде исправления явных ошибок; модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя; модификация в виде частной декомпиляции программы для достижения способности к взаимодействию с другими программами.

«Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации»
(утв. Генпрокуратурой России)

Понятие модификации разъясняется в п. 9 ч. 2 ст. 1270 ГК РФ - любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык, за исключением адаптации, т.е. внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя
(Уголовное дело N 1-31/2015)

Понятие модификации в судебных решениях разъясняется как корректировка имеющейся информации. Например, в июне 2015 года неустановленное следствием лицо, установив на сервер антивируса "Касперского", находящийся в головном офисе ОАО АКБ "Эльбин", программу удаленного доступа и получив таким образом доступ к системе работы банкоматов, модифицировало программу "Кадиаг", установленную в банкоматах, которая позволяет проводить тестовую выдачу денежных средств внутри банкомата, таким образом, чтобы деньги, хранящиеся внутри банкомата, выдавались наружу, в результате чего получило возможность получения информации о количестве денег в банкоматах и завладения ими.

После чего Ганичев О.П. позвонил неустановленному следствием лицу, который, имея возможность удаленно управлять работой банкоматов с помощью модифицированной программы "Кадиаг", дал команду на выдачу денег из банкоматов. Соответственно, понятие модификации компьютерной информации необходимо рассматривать как внесение изменений в уже существующую информацию (Уголовное дело N 1-67/2014)

Например, Ф. осужден за то, что, имея прямой умысел, направленный на хищение чужого имущества, путем модификации компьютерной информации, осознавая общественную опасность своих действий, предвидя возможность и неизбежность наступления общественно опасных последствий и желая этого, с целью незаконного завладения денежными средствами, принадлежащими ОАО "Вымпел-Коммуникации", находясь в офисе продаж Воронежского филиала ОАО "ВымпелКом", путем обмана получил доступ к рабочему компьютеру указанного офиса, на котором установлена программа "Customer Care Back Office" ("ССВО"), данные которой ему стали доступны после ввода заведомо известных ему персональных учетных данных (логина и пароля) действующего сотрудника ОАО "ВымпелКом" -

Затем Ф., имея навыки, полученные им в период работы в должности специалиста обслуживания и продаж ОАО "ВымпелКом", внес 12 корректировок (изменений) в программу, в результате чего перечислил 7080 руб. на баланс находящейся в его распоряжении СИМ-карты. В представленном примере виновным вводилась информация для внесения изменений в программу. В этом случае ввод информации охватывается понятием модификации и самостоятельного значения не имеет.

Учитывая, что модификация всегда сопряжена с вводом информации, данные понятия необходимо отграничивать. Как верно указывается в научной литературе, при вводе информации как отдельном способе преступления создается новый электронный документ (например, SMS-сообщение или электронное платежное поручение) по определенному адресу, в который вносятся данные об увеличении денежной суммы виновного и, соответственно, об уменьшении этой суммы у потерпевшего. В случае модификации компьютерной информации ввод компьютерной информации сочетается с удалением (всей или части) или сохранением (полностью) имеющейся компьютерной информации в уже созданном документе.

# Иное вмешательство

Иное вмешательство – не включает в себя ввод, удаление, блокирование, модификацию информации. Иное вмешательство указывается законодателем для того, чтобы оно охватывало иные последствия неправомерного доступа. Иное вмешательство – изменение информации, хранящейся в компьютере, приведение ее или компьютерной программы в негодное состояние, вывод из строя компьютерного оборудования, разрушение компьютерной системы или машинного носителя, порча информационных ресурсов и тд.

# Пример иного вмешательства

Например, изготовление дубликатов сим-карт и паролей с последующим их использованием через электронную систему N для завладения денежными средствами путем перечисления на счета и банковские карты различных лиц (Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076).

# Пример иного вмешательства

Б., воспользовавшись служебным положением, имея доступ к единой базе данных ОАО "Сбербанк России", направила SMS-сообщения на единый абонентский номер ОАО "Сбербанк России", с указанием кодовой команды, тем самым осуществила вмешательство в функционирование банковского сервера, на котором хранится информация о счетах клиентов ОАО "Сбербанк России". В связи с чем денежные средства с банковского счета К., открытого в ОАО "Сбербанк России", были перечислены на счет абонентского номера, принадлежащего Б., которая впоследствии распорядилась похищенными денежными средствами по своему усмотрению.

# Пример иного вмешательства

В приведенном случае в качестве способа совершения мошенничества указано вмешательство в функционирование средств хранения, обработки, передачи компьютерной информации, поскольку виновное лицо, имея доступ к базе данных через свой сотовый телефон, осуществило операции ввода компьютерной информации - перевод денежных средств с одного банковского счета на другой.

Уголовное дело N 1-102/2013

# Удаление информации

Законодатель не дает определения понятия «удаление информации».

Под ним можно понимать – совершение действий, в результате которых становится невозможно восстановить содержание компьютерной информации, и(или) в результате которых уничтожаются носители компьютерной информации.

Понятия удаления и блокирования приводятся в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных». В данном законе речь идет об уничтожении, но по сути это и есть удаление.

Согласно ст. 3 упомянутого закона

Уничтожение – действия, в результате которых становится невозможным восстановить содержание информации.

Блокирование – временное прекращение сбора, систематизации, накопления, использования, распространения данных, в том числе их передачи и обработки.

Например, Ларин, будучи осведомленным о порядке и правилах доступа к автоматизированной системе и возможности перевода с ее помощью денежных средств без использования банковской карты владельца счета, действуя незаконно, путем обмана, под предлогом перечисления денежных средств на счет владельца банковской карты получил идентификационные данные карты. Продолжая осуществлять свой преступный умысел, Ларин, находясь в офисе сети продаж, обратился к специалисту с требованием о замене СИМ-карты по причине утери прежней. Специалист произвел замену, выдав новую СИМ-карту, что повлекло за собой автоматическое вмешательство в функционирование средства хранения, обработки и передачи компьютерной информации, а именно СИМ-карты, в виде ее блокировки.

Ларин произвел посредством ввода и передачи компьютерной информации, содержащейся в СМС-сообщениях сотового телефона, в информационно-телекоммуникационной сети оператора сотовой связи перевод денежных средств. Своими действиями Ларин путем ввода и блокирования компьютерной информации, используя дубликат СИМ-карты, являющейся средством хранения компьютерной информации, подключенной к автоматизированной системе, совершил хищение с помощью произведенных операций по перечислению денежных средств. В данном примере активация дубликата СИМ-карты прекратила доступ к информации, содержащейся на первоначальной карте, что соответствует понятию блокирования.

# Момент окончания преступления

Последствия для собственника

При хищении чужого имущества

С момента, когда указанное имущество поступило в незаконное владение виновного или других лиц и они получили реальную возможность пользоваться или распорядиться им по своему усмотрению.

Ущерб может причиняться как владельцу счета, так и банку.

При приобретении права на чужое имущество

С момента возникновения у виновного юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом как своим собственным.

# Момент окончания преступления (безналичные средства)

С момента зачисления денег на банковский счет лица оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению, например осуществлять расчеты от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были перечислены в результате мошенничества. В указанных случаях преступление следует считать оконченным с момента зачисления этих средств на счет лица, которое путем обмана или злоупотребления доверием изъяло денежные средства со счета их владельца, либо на счета других лиц, на которые похищенные средства поступили в результате преступных действий виновного.

# Момент окончания преступления

Последствия для компьютерной информации:

- Удаление информации;
- Блокирование информации;
- Модификация информации

## Средства хранения, обработки или передачи

При определении средств хранения, обработки или передачи компьютерной информации исследователями часто используется принцип перечисления возможных технических устройств, предназначенных для хранения информации (например, жесткие диски, оптические диски, карты памяти и т.д.). Однако отсутствие понятия средств хранения, обработки или передачи компьютерной информации вызывает трудности в правоприменительной деятельности.

## Средства хранения, обработки или передачи

Так, в отдельных научных источниках к этим средствам относят кассовые аппараты. Однако кассовые аппараты бывают фискальные и нефискальные. Фискальные кассовые аппараты отличаются от нефискальных наличием фискальной памяти - носителя информации, данные из которого нельзя удалить. В фискальной памяти накапливаются данные об операциях, совершенных при помощи данного кассового аппарата. Те аппараты, в которых отсутствует блок памяти (например, чекопечатающие машинки), нельзя отнести к средствам хранения информации.

## Средства хранения, обработки или передачи

Таким образом, под средствами хранения, обработки или передачи компьютерной информации должны пониматься не любые устройства, а только те, которые предназначены для целей хранения, обработки компьютерной информации и снабжены соответствующим программным обеспечением (блоком памяти). К таким устройствам относят не только стационарные или переносные (ноутбуки, планшеты и т.п.) ЭВМ, но и мобильные телефоны, смартфоны, платежные терминалы и т.п.

См.: Федеральный закон от 22 мая 2003 г. N 54-ФЗ "О применении контрольно-кассовой техники (ККТ) при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт».

## Средства хранения, обработки или передачи

**Загиров И.Е.** обвиняется в совершении преступлений, предусмотренных ст.ст. 272 ч.1 УК РФ, 183 ч.1 УК РФ, 272 ч.1 УК РФ, 273 ч.1 УК РФ, 183 ч.3 УК РФ, 165 ч.1 УК РФ,

Загиров И.Е. совершил преступления, при следующих обстоятельствах.

Руководствуясь корыстным мотивом, преследуя цель личного обогащения, Загиров И.Е., действуя умышленно и осознавая, что без использования абонентской карты и заключения абонентского договора, не обладает правом доступа к компьютерной информации ОАО «...», а именно, ... сообщениям, имея специальные познания и опыт работы с ЭВМ, решил совершить неправомерный доступ к указанной компьютерной информации ОАО «...», то есть информации в системе ЭВМ, с последующим ее копированием.

# Средства хранения, обработки или передачи

Так, Загиров И.Е., находясь в г.Сыктывкаре, в 2007 году, точная дата и время предварительным следствием не установлены, при неустановленных обстоятельствах, приобрел ресивер марки «...» , спутниковую антенну и конвертер, далее, находясь по адресу своего проживания в 19 часов 02 минуты 11 декабря 2009г. во исполнение преступного умысла, направленного на неправомерный доступ к компьютерной информации и копирование информации в системе ЭВМ, установил на ресивер программу неизвестного производителя таким образом, модифицировав программное обеспечение указанного ресивера, в результате чего ресивер стал способен принимать ключи для декодирования закрытых спутниковых каналов . Данное программное обеспечение Загиров И.Е. получил из неустановленных источников в телекоммуникационной сети Интернет .

# Средства хранения, обработки или передачи

- Загиров И.Е., реализуя свой преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации произвел монтаж и настройку приобретенного им комплекта спутникового оборудования . Далее Загиров И.Е., в завершение технического обеспечения неправомерного доступа к охраняемой законом компьютерной информации ОАО «...» подключил антенну к ранее перепрограммированному им спутниковому тюнеру . В последующем Загиров И.Е. по окончании установки оборудования, убедился, что на телевизоре, отображаются закрытые спутниковые каналы ОАО «...» . Таким образом, Загиров И.Е. обеспечил себе возможность просмотра закрытых спутниковых каналов ОАО «...» без заключения соглашения на предоставление услуг с ОАО «...» .

## Хищение права на имущество. По ст. 159.6 УК квалифицируются:

Использование подложного (от имени владельца счета) электронного платежного поручения, направляемого через систему «Банк-Клиент». С объективной стороны это предполагает проникновение помимо санкции банка в его компьютерную систему, ввод и (или) модификацию циркулирующей в ней компьютерной информации, что влечет перечисление
безналичных денежных средств на счет виновного или иной счет, средствами на котором он может воспользоваться как своими;

## По ст. 159.6 УК квалифицируются:

Использование:

программы дистанционного банковского обслуживания счета, примененной для несанкционированной модификации компьютерной информации. С помощью программы виновные направляют подложное платежное поручение о перечислении денег на те счета, средствами на которых они имеют реальную возможность распорядиться в пользу виновного или других лиц;

вредоносной компьютерной программы, обеспечивающей замену файла платежного поручения, направленного посредством электронной системы «Банк-Клиент» владельцем денег на счете в банке на файл, содержащий подложное поручение и реквизиты счета, подконтрольного уже виновному;

## По ст. 159.6 УК квалифицируются:

Использование:

банковской карты организации, дающей возможность несанкционированного отдаленного доступа к управлению расчетным счетом организации и перечисления с данного счета путем вмешательства в функционирование банковских средств хранения, обработки или передачи компьютерной информации денежных средств (за исключением случая хищения их в наличной форме);

фиктивных трудовых договоров, внесения на их основе подложных сведений в табели учета рабочего времени «мертвых душ», предоставления их в электронной форме в бухгалтерию с последующим перечислением заработной платы, начисленной на фиктивно трудоустроенных лиц, на подконтрольные виновному банковские счета;

## По ст. 159.6 УК квалифицируются:

Использование:

не заблокированной или ошибочно подключенной к номеру телефона услуги «Мобильный банк», оказываемой в сфере компьютерной информации и предоставляющей право распоряжаться денежными средствами, находящимися на счете владельца телефонного номера;

кредитных карт, оформленных через электронную программу «Кредитный брокер» на физических лиц, ранее приобретавших товары в кредит. Преступники используют их личные данные, сохранившиеся в системной памяти базы торговой организации. После активирования карт деньги обналичиваются через банкомат;

## По ст. 159.6 УК квалифицируются:

Использование:

полученных путем использования вредоносных программ логинов и паролей, с помощью которых владелец счета управлял движением безналичных денежных средств, для направления в банк через сеть Интернет распоряжения о перечислении средств на подконтрольные виновному счета в другом или том же банке;

полученных по поддельной доверенности дубликата сим-карты номера сотового телефона гражданина и информации о его банковских счетах для несанкционированного входа в компьютерную программу удаленного доступа к счетам клиентов –«Банк Онлайн» — и направления распоряжения о перечислении средств на подконтрольный виновному счет

# Другие виды преступлений в сфере компьютерной информации

**Ст. 272 УК РФ -** Неправомерный доступ к компьютерной информации.

**Ст. 273 УК РФ -** Создание, использование и распространение вредоносных компьютерных программ.

**Ст. 274 УК РФ -** Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

**Статья 272. Неправомерный доступ к компьютерной информации**

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

## Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

## Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

# Дополнительная квалификация

Дополнительная квалификация требуется:

- Для применения более строгой санкции к преступнику;
- В случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для ЭВМ, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ.

В судебной практике нет единообразия по этому вопросу.

# Дополнительная квалификация

Материалы уголовного дела № 1-141/14 в отношении Гимельфарба обвиняемого в совершении преступлений, предусмотренных ч. 3 ст. 272 (19 эпизодов), ч. 3 ст. 159.6 (19 эпизодов) УК РФ,

У С Т А Н О В И Л:

Гимельфарб П.Д. совершил неправомерный доступ к охраняемой законом компьютерной информации, что повлекло модификацию компьютерной информации, совершенное лицом с использованием своего служебного положения

# Новая редакция статьи ст. 159.6 УК РФ

«Хищение чужого имущества путем доступа к электронной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи электронной информации».

Что же касается модификации, блокирования, удаления, копирования и других действий, то все они должны дополнительно квалифицироваться по ст. ст. 272, 273 УК РФ.

# Технологии взлома банковской системы:

1. Эксплойты – вид компьютерной программы, использующей уязвимость программного обеспечения, применимая для проведения атак на вычислительные системы;
2. Удаленное подключение к уязвимым компьютерам для установки вредного программного обеспечения;
3. Зараженное письмо;
4. Шпионская программа, созданная для получения ключей системы дистанционного управления банковскими счетами.

# Действия совершаемые со своей или чужой банковской картой:

1. В случае утраты банковской карты, ее владелец обязан направить соответствующее уведомление банку незамедлительно после обнаружения этого факта. Оператор по переводу денежных средств обязан возместить клиенту сумму операций совершенных без согласия владельца карты.

Ч. 11, 12 ст. 9 ФЗ от 27.06.2011 N161-ФЗ «О национальной платежной системе».

# Действия совершаемые со своей или чужой банковской картой:

2. В случае использования банковской карты без согласия владельца, он обязан направить соответствующее уведомление банку незамедлительно после обнаружения этого факта, но не позднее следующего дня после получения соответствующего сообщения. Оператор по переводу денежных средств обязан возместить клиенту сумму операций совершенных без согласия клиента.

Ч. 11, 12 ст. 9 ФЗ от 27.06.2011 N161-ФЗ «О национальной платежной системе».