ИНФОРМАЦИЯ по профилактике преступлений в ИТТ (*информационно-телекоммуникационные технологии)*

Преступления в сфере информационных технологий или киберпреступность – преступления, совершаемые в сфере и с помощью информационных технологий. Информационно-телекоммуникационные технологии преимущественно используются при совершении преступлений против собственности, а также в сфере незаконного оборота наркотических средств и психотропных веществ. Прокуратура разъясняет о преступлениях в сфере ИТТ.

Преступления в сфере информационных технологий или киберпреступность – преступления, совершаемые в сфере и с помощью информационных технологий. Информационно-телекоммуникационные технологии преимущественно используются при совершении преступлений против собственности, а также в сфере незаконного оборота наркотических средств и психотропных веществ.

Одним из наиболее распространенных преступлений, совершаемых с использованием Интернета, является мошенничество.

Уязвимость внедряемых в финансово-кредитную сферу инновационных технологий и их активное применение на практике эксплуатируют мошенники, совершая посягательства на имущество граждан и организаций.

Распространенный характер носят хищения, связанные с обманом доверчивых граждан. Злоумышленники, представляясь знакомыми, просят о перечислении электронным платежом денежных средств для разрешения сложившейся неблагоприятной жизненной ситуации (к примеру, в связи с ДТП). Нередко преступники представляются сотрудниками правоохранительных органов, а также службы безопасности банков.

Нельзя сообщать по телефону конфиденциальную информацию (персональные данные, номера банковских карт, коды пароли), совершать покупки на непроверенных сайтах. Полученную информацию следует тщательно перепроверять.

Хищения денежных средств граждан все чаще стали совершаться дистанционными способами, путем размещения в открытом доступе на сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров, средства за приобретения которых перечисляются мошенникам.

Так, федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» усилено наказание за хищение денежных средств с банковского счета или электронных денежных средств до 6 лет лишения свободы. При этом уголовная ответственность наступает не только за совершение хищений с использованием банковских карт (их реквизитов и контрольной информации), но и иных электронных средств платежа («электронные кошельки», другие платежные сервисы).

В целях пресечения указанных видов преступлений от граждан требуется предельная внимательность при осуществлении банковских операций с использованием сети Интернет и мобильных телефонов.

За совершения таких деяний предусмотрена уголовная ответственность по ст. ст. 158, 159 УК РФ.

Об уголовной ответственности за хищения персональных данных, денежных средств в сфере и с использованием информационно-телекоммуникационных технологий (далее – ИТТ) и меры предосторожности.

Стремительный рост числа преступлений в сети Интернет свидетельствует о том, что преступники теперь используют цифровую/виртуальную среду также активно, как и реальный мир, что создает для них новую специализацию в преступной сфере: в 2023 году в Российской Федерации было зарегистрировано более 2 миллионов преступлений, из которых более 500 000 (>25%) были преступлениями с использованием ИТТ.

В секторе ИТТ происходят различные преступления, в основном это интернет и мобильное мошенничество с целью хищения денег с банковских счетов граждан ст. 159 УК РФ. Среди других

преступлений — кража с помощью платежных карт (пластиковых карт) — п. «г» 3 ст. 158 УК РФ; производство, использование и распространение вредоносных программ — ст. 273 УК РФ; распространение незаконной информации через интернет — ч. 2 ст. 128.1 УК РФ.

Важным элементом защищенности Ваших персональных данных и денежных средств являются знания.

Для этого рассмотрим некоторые из наиболее распространенных техник, используемых злоумышленниками в сфере ИТТ. К ним относятся:

1. Фишинг — вид интернет-мошенничества, который используют для получения доступа к личной информации пользователя: логинам, паролям, номерам телефонов, данным банковских карт и так далее посредством массовых рассылок электронных писем на электронную почту, текстовых сообщений.
2. Вишинг (голосовой фишинг) — это специальное манипулирование телефонными сетями с целью получения личной и финансовой информации жертв. После создания копии системы банка жертву просят (предпочтительно через поддельное электронное письмо) позвонить по номеру банка для подтверждения деталей.
   Система банка копирует и отклоняет данные, введенные жертвой.
3. SMS-мошенничество — мошенники рассылают SMS-сообщения о транзакциях жертвы (блокировка банковских счетов и кредитных карт) и просят потерпевшего сообщить данные счета и пароли в полученном SMS-сообщении, что приводит к хищению средств;
4. Мошенничество с предоплатой — покупка и продажа товаров на разнообразных сайтах (Юла, Avito.ru и др.),
5. Поиск работы (JOB.ru, HH.ru или интернет ресурсы RABOTA.ru, HeadHunter.ru и др.);
6. Взлом аккаунтов в социальных сетях и отправка сообщений друзьям и знакомым с требованием денег — мошенники пользуются беспечностью людей и используют специальное программное обеспечение для входа в аккаунты в социальных сетях и отправки сообщений всем знакомым от имени

взломанного пользователя с описанием сложной жизненной ситуации и просят финансовой помощи или одолжить денег;

7. Мошенники, выдающие себя за сотрудников полиции или следователей, сообщают родственникам жертв, что те подозреваются в совершении несчастного случая или преступления, и предлагают им иммунитет от судебного преследования, если они переведут определенную сумму денег на указанный счет;
8. Участие в онлайн-опросах, сообщение о выигрышах в лотерею и компенсация за ранее оказанные услуги — мошенники предлагают крупные суммы денег пользователям Интернета, которые участвовали в онлайн-опросах или сообщили о выигрыше в лотерею. Иногда требуется «депозит» для получения соответствующих документов или уплаты пошлины.

Как нужно действовать, чтобы не дать злоумышленнику похитить Ваши персональные данные, денежные средства?

В случае если к вам обратились по сотовой связи или же в онлайн, и под разными поводами пробуют признать данные о вашей банковской карте, пароли или же иную индивидуальную информацию, будьте аккуратны: это видимые симптомы действий злоумышленников.

Если у Вас появились подозрения, советуем закончить общение и как можно быстрее связаться с банком по телефонному номеру, обозначенному на оборотной стороне вашей банковской карты. Не следуйте рекомендациям третьих лиц.

Сохраняете вашу карту в недоступном от посторонних людей месте.
В случае если совершено хищение с Вашей банковской карты, немедленно пишите заявление в ближайший отдел полиции.

Уважаемые граждане, ни в коем случае не наносите информацию на банковскую карту о код-пароле (пин-код) для доступа к банковской карте посредством терминала, не храните такую информацию в непосредственной близости с банковской картой в виде записей на листе и тому подобное. Такие действия создают беспрепятственную возможность для злоумышленников по обналичиванию денежных средств с банковского счета.

При заявлении в полицию необходимо приложить копию выписки счета, полученную предварительно в банке, где станет заметно перемещение денежных средств по счету. Кроме того, возможно обеспечить детализацию телефонных звонков и смс, это в случае, если хищение денежных средств произошло методом телефонной связи.

ОСНОВНЫЕ АКТУАЛЬНЫЕ СХЕМЫ МОШЕННИЧЕСТВА В СФЕРЕ ИТТ

1. Получение кода из СМС, дальнейший обман через телефонные звонки (двухэтанная схема, основная).
Поступает звонок от якобы сотрудника правоохранительных органов, банка, оператора связи или иных должностных лиц. Под различными предлогами (продление договора об оказании услуг связи, продление полиса ОМС, запись к врачам или полученные результаты проведенных анализов, электронная очередь в поликлинику, электронный дневник, передача показаний за коммунальный услуги, запись на замену счетчиков и т.д.) убеждают продиктовать код из СМС.

После чего:

- взламывают Госуслуги, получают персональные данные, оформляют кредиты и т.д.
- поступают звонки о том, что мошенники воспользовались кодом из СМС и взломали Госуслуги / получили доступ к персональным данным / денежные средства в опасности / оформили кредиты / осуществляется перевод денег ВСУ. В связи с чем, чтобы обезопасить свои деньги необходимо перевести их на безопасный счет / оформить кредит и перевести их потом на безопасный счет / передать внештатному сотруднику наличные и т.д.

2. Обман через телефонный звонок - «финансирование ВСУ, декларирование денежных средств».
Поступает звонок от сотрудника ФСБ / прокуратуры / Росфинмониторинга о том, что со счета гражданина осуществляется финансирование ВСУ / денежные средства необходимо задекларировать.

После «обработки» гражданина убеждают перевести / передать деньги.

3. Создание поддельных аккаунтов руководителей, использование искусственного интеллекта.
Мошенники создают аккаунт в мессенджерах Вотсап, Телеграм и других визуально похожийна аккаунт руководителя, с которого работникам организации направляют сообщение о необходимости связаться, например, с сотрудником полиции, от которого узнают о попытке хищения с их счета денег или переводе на счет террористической организации, чему можно противодействовать, переведя деньги на «безопасный счет».

Также обманывают и убеждают при помощи сгенерированного с помощью искусственного интеллекта голоса / изображения руководителя / известного должностного лица (например, Губернатора г. Санкт-Петербурга).

4. Создание фишинговых сайтов.
После того, как покупатель связывается с продавцом, его убеждают в наличии товара и просят внести частичную либо полную оплату товара. В целях убеждения в реальности сделки продавец может направить покупателю фото документов об отправке товара почтой России, СДЭК или другой организацией. После получения денег товар могут не отправить или отправить не того качества и не по цене договора.

Также распространены случаи переходов по ссылкам для оплаты на таких сайтах и списание денежных средств со счета потерпевшего.

5. Поддельные квитанции.
Мошенники подделывают квитанции об оплате коммунальных услуг. После оплаты по QR-коду деньги уходят на счета мошенников.

Преступления в сфере информационных технологий или **киберпреступность** — преступления, совершаемые в сфере электронных информационных технологий.

К киберпреступлениям относятся такие общественно опасные деяния, которые совершаются с использованием средств

компьютерной техники в отношении информации, обрабатываемой и используемой в кибернетическом пространстве [1].

Понятие и признаки киберпреступлений

Под кибернетическим преступлением понимается виновное противоправное деяние (действие или бездействие) субъекта, совершенное в кибернетическом пространстве с использованием сетей компьютера, запрещенное действующим законодательством под угрозой наказания[2].

Российский учёный И. М. Рассолов в своих работах отмечает следующие признаки киберпреступлений:

1. Использование сетей компьютера и международного информационного обмена, являющееся главной особенностью преступления в сфере высоких технологий. При этом компьютер и его сети выступают качестве предмета преступления, орудия преступления или средства, на котором подготавливаются противоправные деяния.

2. Транснациональный характер рассматриваемых преступлений (они совершаются глобальном информационном пространстве) и интернациональность участников преступного сообщества.

3. Устойчивая тенденция к «организованности» киберпреступлений и выход их за национальные рамки.

4. Наличие преступной пирамиды, состоящей как минимум из трех уровней взаимодействия[2].

Виды

Преступления в сфере информационных технологий включают как распространение вредоносных программ, взлом паролей, кражу номеров банковских карт и других банковских реквизитов, фишинг, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду, и т. п.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем[3].

Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество. Так, в письме Федеральной комиссии по рынку ценных бумаг от 20 января 2000 г. №ИБ-02/229 указывается, что инвестирование денежных средств на иностранных фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлечёнными в различного рода мошеннические схемы. В России, по данным на 2020 год, 70,6 % киберпреступлений — это мошенничество. Самый распространенный вид киберпреступлений — звонки по телефону, когда мошенники пытаются узнать у владельцев банковских карт конфиденциальные данные, сделать перевод или установить программы удаленного доступа.[4]

Другой пример мошенничества — интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.

В различных государствах, в частности США, получили распространение аферы, связанные с продажей доменных имён: производится массовая рассылка электронных сообщений, в которых, например, сообщают о попытках неизвестных лиц зарегистрировать доменные имена, похожие на адреса принадлежавших адресатам сайтов, и владельцам сайтов предлагается зарегистрировать ненужное им доменное имя, чтобы опередить этих лиц. Так, вскоре после 11 сентября 2001 года Федеральная торговая комиссия США отметила факт массовой продажи доменных имён зоны «usa».

Киберпреступления в финансовой сфере в 2024 году

В третьем квартале 2024 года банки предотвратили 16,1 миллиона кибератак на счета клиентов, предотвратив хищения на сумму 4,9 триллиона рублей. Это в три раза больше, чем годом ранее, что указывает на значительный рост масштабов кибермошенничества.Несмотря на усиленные меры защиты, преступникам удалось похитить рекордную сумму в 9,3 миллиарда рублей за третий квартал 2024 года. Более 40% этой суммы было украдено через онлайн-банкинг и денежные переводы, что отражает смещение фокуса мошенников с операций по банковским картам.

25 июля 2024 года вступил в силу новый закон о механизмах борьбы с мошенничеством, который уточнил понятие "авторизованного мошенничества". Это ситуации, когда жертву манипулируют для добровольного перевода денег под ложным предлогом.Банк России активно борется с мошенническими ресурсами. В третьем квартале 2024 года регулятор инициировал блокировку 12 100 мошеннических веб-сайтов и страниц в социальных сетях, а также передал информацию о 42 100 мошеннических телефонных номерах операторам связи.Эти данные демонстрируют растущую сложность и масштаб киберпреступлений в финансовой сфере, а также усиление мер противодействия со стороны регулирующих органов и финансовых учреждений.[5][6][7][8]

Уголовная ответственность в странах мира

Россия

Данная группа посягательств является институтом особенной части уголовного законодательства, ответственность за их совершение предусмотрена гл. 28 УК РФ[9]. В качестве самостоятельного института впервые выделен УК РФ 1996 года. и относится к субинституту «Преступления против общественной безопасности и общественного порядка». Видовым объектом рассматриваемых преступлений являются общественные отношения, связанные с безопасностью информации и систем обработки информации с помощью ЭВМ.

По УК РФ преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), [[нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей]] (ст. 274 УК РФ). В 2012 году в УК РФ были введены статьи, регламентирующие уголовную ответственность за различные виды кибермошенничества (статьи 159.3 и 159.6 УК РФ), формально не относящиеся к 28 главе Уголовного кодекса.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) совершаются только путём действий, в то время как [[нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей]] (ст. 274 УК РФ) — путём как действий, так и бездействием.

Неправомерный доступ к компьютерной информации и нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ — с формальным. В качестве последствий в ст. 272 и 274 УК указываются: уничтожение, модификация, блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т. п.

В России борьбой с преступлениями в сфере информационных технологий занимается УБК МВД России и отделы региональных управлений внутренних дел.

Германия

В Германии к преступлениям в сфере оборота компьютерной информации относятся: — действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены

или переданы электронным, магнитным или иным способом (§ 202a); — нарушение тайны телекоммуникационной связи (§ 206); — действия лиц, учиняющих подделку или использующих поддельные технические записи, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§ 268); — аналогичная подделка данных, имеющих доказательственное значение (§ 269); — действия лиц, уничтожающих, изменяющих или утаивающих технические записи (§ 274); — действия лиц, противоправно аннулирующих, уничтожающих, приводящих в негодность или изменяющих данные (§ 303a); — действия лиц, нарушающих обработку данных путём разрушения, повреждения, приведения в негодность установки для обработки данных или носителей информации (§ 303b). — незаконное вмешательство в деятельность телекоммуникационных установок (§ 317).

Кроме того, германское законодательство устанавливает уголовную ответственность за компьютерное мошенничество, под которым понимается умышленное деяние с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путём воздействия на результат обработки данных путём неправильного создания программ, использования неправильных или данных, неправомочного использования данных или иного воздействия на результат обработки данных (§ 263a).

Люксембург

Нормы о киберпреступлениях содержатся в ст. ст. 509-1, 509-2, 509-3, 524 УК Люксембурга.

Статья 509-1 УК Люксембурга предусматривает ответственность за неправомочный доступ к системе или части системы обработки данных и незаконное пребывание в такой системе. Санкция за это преступление предусмотрена в виде штрафа или заключения на срок от 2 месяцев до года. Если указанные действия повлекли изменение или уничтожение данных, содержащихся в системе, то верхний предел срока заключения увеличивается до 2 лет.

Статья 509-2 запрещает преднамеренное затруднение или изменение функционирования системы автоматической обработки

данных. Наказание — штраф или лишение свободы на срок от 3 месяцев до 3 лет.

Статья 509-3 направлена на охрану целостности и качества данных. Она устанавливает, что лицо, умышленно и без надлежащих полномочий вводящее данные в электронную систему их обработки, удаляющее или изменяющее данные, находящиеся в этой системе, изменяющее действие системы или способ передачи данных, подлежит уголовной ответственности (штраф или заключение на срок от 3 месяцев до 3 лет). Согласно ст. 524 УК Люксембурга, любое вмешательство в телекоммуникации является преступлением, за которое лицо может быть подвергнуто штрафу или заключению от 1 месяца до 3 лет.

Международное сотрудничество

Преступления в сфере информационных технологий очень часто являются международными, то есть преступники действуют в одном государстве, а их жертвы находятся в другом государстве. Поэтому для борьбы с такими преступлениями особое значение имеет международное сотрудничество.

Конвенция Совета Европы о преступности в сфере компьютерной информации ETS № 185 была подписана 23 ноября 2001 г. в Будапеште[10].Она открыта для подписания как государствами — членами Совета Европы, так и не являющимися его членами государствами, которые участвовали в её разработке. В частности, её подписали США и Япония. Россия на настоящий момент не подписала Конвенцию[11].

Конвенция Совета Европы о киберпреступности подразделяет преступления в киберпространстве на четыре группы.

- В первую группу преступлений, направленных против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст. 2), незаконный перехват (ст. 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) (ст. 4) или системы (ст. 5). Также в эту группу преступлений входит противозаконное использование

специальных технических устройств (ст. 6) — компьютерных программ, разработанных или адаптированных для совершения преступлений, предусмотренных в ст. 2 — 5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерной системе в целом или любой её части). Нормы ст. 6 применимы только в том случае, если использование (распространение) специальных технических устройств направлено на совершение противоправных деяний.

- Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст. 7 — 8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных.
- Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение порнографии, эротики и детской порнографии, а также владении детской порнографией, находящейся в памяти компьютера (ст. 9).
- Четвертую группу составляют преступления, связанные с нарушением авторского права и смежных прав.

Согласно Конвенции, каждое государство-участник обязано создать необходимые правовые условия для предоставления следующих прав и обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, её части или носителей; изготовление и конфискация копий компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Конвенция также требует создать необходимые правовые условия для обязания интернет-провайдеров проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся

технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В начале 2002 г. был принят Протокол № 1 к Конвенции о киберпреступности, добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающегося на расовой, национальной, религиозной или этнической принадлежности.

Критика Конвенции о киберпреступности

Ряд общественных организаций подписались под совместным протестом против принятия вышеуказанной Конвенции. В их число вошли международная организация Internet Society, организации Electronic Frontier Foundation (США), Cyber-Rights & Cyber-Liberties (Великобритания), Kriptopolis (Испания) и другие. Авторы обращения возражают против положений, требующих от провайдеров Интернета вести записи о деятельности их клиентов. Во введении ответственности провайдеров за содержание информации авторы усматривают «бессмысленную обузу, которая поощряет слежку за частными коммуникациями». В обращении отмечается также, что положение об обеспечении государственных органов шифровальными ключами может стать основанием для свидетельствования пользователей против самих себя, что противоречит статье 6 Европейской конвенции о защите прав человека.

Общественность, кроме того, выступает против того, что за нарушение авторских прав должна непременно следовать уголовная ответственность.

См. также

- Интернет-преступность
- Компьютерный терроризм
- Информационное право
- Несанкционированный доступ

Примечания

1. И.М. Рассолов. Право и Интернет. Теория кибернетического права. Монография. М. : Норма, 3-е изд. 2021. Дата обращения: 8 августа 2025. Архивировано 8 декабря 2024 года.
2. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 427 с. — ISBN 978-5-534-18043-5. Дата обращения: 8 августа 2025. Архивировано 31 мая 2025 года.
3. Впервые в мире хакеры атаковали водопровод. Дата обращения: 20 ноября 2011. Архивировано 22 ноября 2011 года.
4. Преступность. Статистика проблемы в России и регионах. *Если быть точным*. Дата обращения: 13 августа 2021. Архивировано 22 июля 2021 года.
5. *Билык, Кирилл.* ЦБ выявил почти 25 тыс. мошеннических ресурсов за полгода. *rb.ru* (2024). Дата обращения: 24 декабря 2024. Архивировано 24 декабря 2024 года.
6. НОТА МОДУС. *modus.nota.tech*. Дата обращения: 24 декабря 2024. Архивировано 19 ноября 2024 года.
7. *ЦБ в III квартале инициировал блокировку 12,1 тысячи мошеннических сайтов. РИА Новости. 9 декабря 2024. Архивировано 24 декабря 2024. Дата обращения: 24 декабря 2024.*
8. Ущерб от киберпреступлений в 2024 году составил 99 млрд рублей - Новости - Управление рисками и комплаенс. *https://x-compliance.ru* (2024). Дата обращения: 24 декабря 2024. Архивировано 24 декабря 2024 года.
9. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. 17.06.1996. № 25. Ст. 2954. (с послед. изм. и доп.)
10. Convention on Cybercrime. Дата обращения: 25 февраля 2015. Архивировано 11 августа 2011 года.
11. Распоряжение Президента РФ от 22.03.2008 № 144-рп "О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о киберпреступности»