**Ответственность за киберпреступления.**

Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

**Что такое киберпреступление?**

появилось огромное количество весьма пространственных определений, но суть всех их сводится к следующему: **«киберпреступление – это любое преступление в электронной сфере, совершенное при помощи компьютерной системы или сети, или против них»**.

Удалось выявить и *особенности данного вида преступлений*, это:

- чрезвычайная скрытность деяний, которая достигается применением механизмов анонимности и шифрования;

- трансграничность, преступник и жертва могут быть разделены тысячами километров, границами нескольких государств;

- нестандартность способов совершения;

- автоматизированный режим.

**Виды**

Поскольку киберпреступления охватывают широчайший пласт общественных отношений, предполагают использование различного оборудования и имеют целый спектр способов совершения, логично провести их классификацию.

*Конвенцией Совета Европы виды киберпреступлений объединены в пять групп*.

**Первая группа** включает все компьютерные преступления, направленные против компьютерных данных и систем (например, незаконный доступ, вмешательство в данные или системы в целом).

**Вторую группу** составляют противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, получение экономической выгоды иными способами).

Правонарушения **третьей группы** связаны с содержанием данных или контентом.

[Нарушение авторских и смежных прав](https://urist.one/imushhestvo/avtorskie-prava/narushenie-avtorskih-prav.html) относится к **четвертой группе**, выделение определенных [видов преступлений](https://urist.one/dolzhnostnye-prestupleniya/obshhie-opredeleniya/prestuplenie-opredelenie.html) в которой отнесено к законодательству конкретных государств.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в **пятую группу** киберпреступлений.

**Количество киберпреступлений**, совершаемых в России и в мире, неуклонно растет, **за последние пять лет их число колеблется в пределах 8 тыс. – 17 тыс., с ежегодной динамикой около 10%**.

Меняется и их качественный состав, и размер причиненного ущерба.

Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно.

Законодательство большинство стран мира предполагает уголовную ответственность за совершение преступлений данного вида, крупные штрафы, [лишение свободы](https://urist.one/dolzhnostnye-prestupleniya/nakazaniya/lishenie-svobody.html) и даже смертная казнь.

Ответственность за киберпреступления в России предусматривается главой 28 УК РФ и касается только компьютерных преступлений.

В зависимости от тяжести преступления и размера причиненного вреда статьи 272,273 и 274 УК РФ предполагают наказание в виде штрафа от 100 тыс. рублей, [исправительных или принудительных работ](https://urist.one/dolzhnostnye-prestupleniya/nakazaniya/ispravitelnye-raboty.html) от 6 месяцев до 5 лет, ограничения или лишения свободы до 7 лет. Возможно сочетание видов наказания.

В целом можно охарактеризовать российское законодательство в сфере киберпреступности как недостаточно развитое, требующее более детальной проработки и увеличения количества составов, за которые предусмотрена ответственность.

Разработка национальных систем борьбы с данным видом преступности, безусловно, необходима, но локальное расследование киберпреступлений усложняется по нескольким причинам:

требуется специфическое образование и опыт;

часто преступник и жертва находятся в разных странах, а следственные действия правоохранительных органов как раз ограничены пределами одного государства;

преступники имеют возможность выбрать наиболее лояльную правовую систему.

Говоря о России, стоит отметить, что в нашей стране с 1992 год существует Бюро специальных технических мероприятий МВД России.

Сотрудники Бюро, проходят специальную подготовку в лучших технических ВУЗах страны, а также в учебных центрах крупнейших компаний, работающих в IT-отрасли.

**Как защитить себя и близких?**

Вот **несколько конкретных рекомендаций**:

не обращать внимания на звонки и смс, сообщения о выигрышах с незнакомых номеров, никогда не перезванивать на них, не отправлять сообщения;

никому не сообщать реквизиты своей пластиковой карты, со всеми вопросами обращаться непосредственно в отделение банка;

установить надежный антивирус на свои гаджеты и регулярно проводить полную проверку системы.

покупать только лицензионное программное обеспечение.

**Итак**, преступления в электронной сфере получают все большее распространение. Преступникам не страшны границы государств и чужды моральные запреты.

 Несовершеннолетние и киберпреступления

Общепризнанно, что медиасреда предоставляет детям и подросткам как положительные возможности (самореализация, творчество), так и отрицательные (вовлечение подростков в конкретную зависимость и т.д.). К сожалению, медиасреда также может стать некой атмосферой вовлекания подростков в преступные деяния: доведение до самоубийства посредством моббинга, кибермошеничество, хищение денег с электронного родительского кошелька, порнография, знакомство педофилов с несовершеннолетними, свободный доступ к экстремистским сайтам, продажа наркотических веществ через интернет и т.д.

В силу возрастных особенностей, а также в связи с невысокой медиаграммотностью населения, подростки могут стать жертвой киберпреступлений, а порой и превратиться в преступников. Обратим внимание на актуальную в наше время проблему киберпреступности.

Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных [1].

В России 90% преступлений, связанных с киберпреступностью, латентны [1]: практически каждый в нашей стране сталкивался с определенными видами киберпреступлений (вирусы, снимающие деньги с интернет-кошельков, сомнительные письма от банков, просящих предоставить личные данные, смс-сообщения, требующие перечисления финансовых средств по указанному адресу в связи с тем, что родственник попал в тяжелую ситуацию и т.д.). В современное время даже не все взрослые могут разобраться в махинациях, организованных интернет-средой. Особо незащищенной категорией являются дети и подростки, которые в силу возрастной психологии и недостаточности социального опыта могут легко поддаться влиянию мошенников.

Традиционно выделяют 3 вида киберпреступлений: деяния, где программное обеспечение является способом преступлений (похищение информации, несанкционированный доступ, уничтожение или повреждение файлов и устройств и т.п.); действия, где программное обеспечение используются как орудие преступления (электронные хищения и т.д.); преступления, где программное обеспечение играет роль девиантных интеллектуальных средств (например, размещение в интернете порносайтов) [1].

Дети и подростки подвергаются определенной опасности в случаях, связанных с кибермошенничеством (заражение компьютера вирусами, потеря информации с помощью определенных программ, снятие денег с электронных счетов, неконтролируемый доступ к порнографическим сайтам, знакомство педофилов с детьми и подростками).

Таким образом, родителям и образовательным учреждениям стоит озадачиться вопросами, связанными с безопасностью детей и подростков на интернет-просторах. На основании анализа психологической литературы, характеризующей личностные и возрастные особенности подростков [2], **выделим некоторые причины, вследствие которых подростки могут стать объектами или субъектами преступлений:**

**Социально-экономические:** недостаточный воспитательный потенциал школы (неразвитая общественная жизнь, отсутствие мероприятий, выполняющих воспитательную функцию); некорректная профилактика преступлений среди несовершеннолетних; слабая правовая просвещенность относительно наиболее популярных в подростковой среде преступлений; нестабильная ситуация в стране, кризисы.

 **Проблемы социализации:** проблемы в семье (девиантное поведение родителей, неполные семьи, слабое воспитательное воздействие, педагогическая и психологическая неграмотность в воспитании, отсутствие личного контакта с подростками, безразличие и т.д.); проблемы в межличностных отношениях (неумение выстраивать общение со сверстниками, замкнутость); неорганизованность досуговой деятельности подростка;

**Психологические трудности:** доверительное отношение к группе сверстников, возможность получения определенного статуса в группе; опасное любопытство.

Охарактеризуем **возможные преступления**, возникающие в медиасреде. Серьезное распространение в медиасреде получил кибермоббинг, который, по своей сути, является травлей, притеснением партнера по общению. Наиболее опасным его проявлением стало доведение до самоубийства. Анонимность и безнаказанность моббинга в интернет-среде усугубляют риск доведения до суицида некоторых пользователей. Моббинг реализуется в виде угроз, унижения чести и достоинства, издевательств сверстников над подростком-жертвой. Кибермоббинг актуализирует суицидальный риск через оскорбительные смс-сообщения, унизительные сообщения в аккаунтах социальных сетей, выкладывание видео с фиксацией моббинг-процесса над жертвой в социальных сетях и на видеопорталах. Это может спровоцировать у подростка, зачастую имеющего в результате регулярных моббинг-действий ослабленное здоровье и нервную систему, мысли о суициде. Отметим, что данный вид преступлений характеризуется с помощью статьи 110 УК РФ. «Доведение до самоубийства». По мнению юристов, в эту статью следует внести поправки и конкретику, оценивающие подобные преступления, происходящие в медиасреде.

Рассмотрим кибермошенничество – мошенничество, осуществленное с помощью программного обеспечения и интернет-ресурсов. По официальной статистике МВД России за 2014 год зарегистрировано 11000 киберпреступлений [3]. Официальная статистика базируется на поданных заявлениях потерпевших, на самом деле пострадавших от киберпреступлений может быть в разы больше. Известны следующие способы кибермошенничества: 1. Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям). С помощью данного вида преступник сможет узнать всю нужную информацию у доверчивого подростка, а далее использовать ее в своих интересах (требование денежных средств, унижение чести и достоинства, искажение информации). Стоит отметить, что с помощью фишинга «страдать» от потери конфиденциальных данных может не только подросток, но и вся его семья, 2. Шпионские программы, направленные на слежение за объектами киберпреступника. Данный вид преступления также является опасным для всей семьи, так как позволяет контролировать местонахождение не только ребенка или подростка, но и членов его семьи с последующими преступными целями. 3. Обман при покупке товара в интернет-магазине. Глобализация сделала доступным, легким и простым способ приобретения товаров в интернет-среде, что может способствовать созданию фальшивых сайтов, групп в социальных сетях, предлагающих за низкую цену приобрести товары. Нередко такие привлекательные предложения оказываются обманом, в результате которого подросток тратит денежные средства. 4. SMS-мошенничество. Один из наиболее популярных видов получения денежных средств мошенниками. Он направлен не только на детскую, молодежную аудиторию, но и на взрослых и пожилых людей. Такие смс-сообщения обычно содержат следующую информацию: выигрыш в лотерее, выигрыш средства передвижения или недвижимости, сообщение от родственника с просьбой о переводе денег в связи с тяжелой жизненной ситуацией. Цель таких рассылок – получение от доверчивых абонентов денег. Главным намерением кибермошенничества является завладение конфиденциальными данными подростка или его семьи, а также получение денежных средств обманным путем.

Еще одним преступлением в медиасреде, оказывающим угрозу безопасности страны, является вовлечение подростков и молодежи в террористические и экстремистские преступления (по данным Центра Безопасного Интернета 11% подростков посещают экстремистские и националистические ресурсы). В январе - октябре 2015 года на территории Российской Федерации зарегистрировано 1392 преступления террористического характера (+54,3% по сравнению с АППГ) и 1109 преступлений экстремистской направленности (+26,9% по сравнению с АППГ). [4] Экстремизм является одной из наиболее сложных проблем современного российского общества, что связано, в первую очередь, с многообразием его проявлений, неоднородным составом экстремистских организаций, которые угрожают национальной безопасности Российской Федерации. Выделим самые распространенные причины, способствующие вовлечению в террористические и экстремистские организации: религиозный радикализм; проблема женского одиночества; поиск острых ощущений; несформированность ценностно-смысловой сферы; ведомость, конформный тип поведения; любопытство; синдром катарсиса; длительное пребывание в стрессовой ситуации; идеализация маскулинности современных боевиков наряду с отторжением культа феминности современных мужчин; бегство от семейных, межличностных проблем, а также проблем с законом. Абсолютно все из этого перечня усугубляется спецификой медиапространства. Нередко для пропаганды терроризма и экстремизма используют социальные сети: несложно найти группы («ИГИЛ», «Типичный араб», «Arabian TRVP» и др.), распространяющие информацию о современной террористической организации «ИГИЛ», запрещенной в Российской Федерации. Также в социальных сетях выкладываются видеоматериалы с фиксацией терактов, взрывов, разбоев, организованных данной группировкой. В них пропагандируется внутрикультовая музыка, идеализируются фотографии, изображающие любовь девушки к террористам, славится оружие, ведутся призывы к борьбе за псевдосправедливость.

Исходя из описанных проявлений девиантного и делинквентного поведения в медиасреде, выделим **следующие направления обеспечения медиабезопасности**: 1) демонстрация государственной заинтересованности в медиаобразовательных технологиях; 2) внедрение медиаобразования в школе в качестве классных часов и обязательных предметов; 3) предоставление заинтересованным лицам, занимающимся изучением медиаобразования и медиабезопасности, больше возможностей для проведения исследований, организации мероприятий и возможностей повышения медиакомпетентности подрастающего и взрослого поколения.

Также считаем важным разработку программы государственного регулирования распространения медиапродукции, обеспечивающие возможность родительского контроля. **Выделим направления работы с родительским сообществом**: 1) ознакомление с научными данными по медиаобразованию, анализ возможных деструктивных воздействий медиапродукции; 2) развитие медиакомпетентности, критического мышления; 3) формирование интереса родителей к регулярному ознакомлению с научными разработками в области медиабезопасности; 4) стимулирование интереса родителей к анализу медиапродукции, предпочитаемой их детьми.

Несмотря на запрет и обилие нормативно-правовых актов, направленных на борьбу с преступлениями, проследить за соответствием медиасреды издавна сложившимся в обществе нормам и ценностям остается довольно сложно. Государственным структурам, образовательным учреждениям и родительскому сообществу следует уделить внимание профилактике, направленной на превенцию преступлений в медиапространстве.

Эти направления согласовываются с работой среди педагогических коллективов образовательных учреждений: 1) стимулирование интереса у педагогов к медиаобразовательным технологиям; 2) привлечение внимания к проявлениям агрессивного, насильственного поведения подростков, связанного с изображением насилия в СМИ; 3) организация обсуждений с подростками новинок медиапродукции; 4) приглашение специалистов по медиабезопасности в школы; 5) проведение классных часов с родителями по теме опасных деструктивных воздействий медиапродукции, вынесение данной темы на методические собрания педагогов; 6) рассмотрение на уроках гражданства и обществознания положения закона №436 ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», обсуждение принципов маркирования медиасюжетов в соответствии с законом. Несмотря на запрет и обилие нормативно-правовых актов, направленных на борьбу с преступлениями, проследить за соответствием медиасреды издавна сложившимся в обществе нормам и ценностям остается довольно сложно. Государственным структурам, образовательным учреждениям и родительскому сообществу следует уделить внимание профилактике, направленной на превенцию преступлений в медиапространстве. Предложенные рекомендации, минимизируют деструктивные воздействия и преступные деяния в современной медиасреде, повысят уровень медиакомпетентности взрослого и подросткового населения.

Пожалуйста, не забудьте правильно оформить цитату:
Книжникова С. В., Гребёнкина Ю. В. Риск вовлечения детей и молодежи в преступления через медиасреду // Научно-методический электронный журнал «Концепт». – 2016. – Т. 24. – С. 88–93. – URL: <http://e-koncept.ru/2016/56419.htm>.

Следующим опасным явлением в современной медиасреде, с каждым годом набирающим обороты, является открытый и неконтролируемый доступ к порнографическим сайтам и телеканалам (по данным Центра Безопасного Интернета 39% подростков посещают порносайты). Откровенные эпизоды медиапродукции смакуются и в фильмах («Муви 43», «Мачо и ботан 2», «Домашнее видео», «Superнянь», «50 оттенков серого»), клипах («Санта Лючиа», скандальных клипах Miley Ray Cyrus или Britney Jean Spears), телепередачах («Дом-2», «Топ-модель по-американски», «Холостяк»). Это таит в себе опасности приобщения подростков к раннему сексуальному опыту, промискуитету и использованию сексуальных связей для достижения каких-либо целей. В продолжение темы напомним, что в 2014 году уполномоченный при Президенте РФ по правам ребенка П.Астахов обратил внимание на то, что на 35,6% выросло число детей, признанных потерпевшими от преступлений против половой неприкосновенности. Пострадавших из-за понуждения к действиям сексуального характера (ст. 133 УК РФ) стало больше на 162,5%, половых сношений и других действий сексуального характера (ст. 134 УК РФ) – на 121%, изнасилований (cт. 131 УК РФ) – на 28,3%, насильственных действий сексуального характера (ст. 132 УК РФ) – на 24,4%, развратных действий (cт. 135 УК РФ) – на 15,6%. По статистике вышедшие из тюрьмы педофилы становятся рецидивистами в 98% случаев. Таким образом, для преступлений сексуального характера в отношении несовершеннолетних характерна динамика. В силу анонимности медиасреды данный вид преступлений стало проще реализовать: педофилы выстраивают отношения с подростками на чатах, форумах, в социальных сетях. Преступники знакомятся с подростками, позиционируя себя как будущего хорошего друга, старшего товарища, помощника. После установления контакта с несовершеннолетними преступники могут предложить личные встречи, предложить отправлять фотографии обнаженного, эротического характера, интимное общение через веб-камеру.