СТОП УГРОЗА

ШКОЛА БЕЗОПАСНОСТИ

# ИНТЕРНЕТ-БЕЗОПАСНОСТЬ БЕЗ ПРОБЛЕМ

## СОВМЕСТНЫЙ ПЛАН ДЛЯ ПЕДАГОГОВ, РОДИТЕЛЕЙ И ДЕТЕЙ

16+

Москва 2020

Анисимов А.В.

# Интернет-безопасность без проблем. Совместный план для педагогов, родителей и детей

«ЛитРес: Самиздат»

2020

**Анисимов А.В.**

Интернет-безопасность без проблем. Совместный план для педагогов, родителей и детей / Анисимов А.В. — «ЛитРес: Самиздат», 2020

Методические рекомендации подготовлены в помощь педагогам образовательных организаций. В книге вы найдёте анализ типичных проблем с интернет-безопасностью у учащихся и пути их решения, информацию для педагогов начальной школы, среднего и старшего звена, методический материал для взаимодействия педагога с подростками, законными представителями, представителями общественности, специалистами по интернет-безопасности, сотрудниками правоохранительных органов, а также список дополнительной литературы.

# Содержание

# Введение

Интернет представляет собой всемирную систему объединенных компьютерных сетей для хранения, обработки и передачи информации. В начале 1970-х годов интернет был достоянием небольшого числа людей. В США даже издавался справочник пользователей сети Интернет. С тех пор количество пользователей возросло в тысячи раз, и существование такого справочника не представляется возможным. Его толщина сегодня составила бы 116 километров. Увеличение вычислительной скорости компьютеров, ширины каналов связи, емкости хранения данных позволили многократно повысить возможности сети Интернет и привлечь значительно большее число пользователей. Сегодня только в России насчитывается более 80 миллионов пользователей Сети.

Современная ситуация развития общества характеризуется быстрыми изменениями во всех его сферах. Основой трансформации современного общества являются цифровые технологии, которые обеспечивают высокую скорость распространения информации, создают условия для публичной информационной открытости всех сфер жизни, высокой скорости принятия решений на всех уровнях управления государства, общества и производства, информатизации бизнес-процессов, автоматизации рутинного интеллектуального труда, постоянного обновления программного обеспечения, оборудования и технологий. Происходят кардинальные изменения в мире навыков, квалификаций и профессий, возможностей личности в разных видах деятельности.

Изменения происходят и в системе образования. Появляются новые технологии обучения (цифровые, сетевые, интернет-технологии), новые системы оценки качества знаний. В рамках федерального проекта «Цифровая образовательная среда» поставлена цель создания условий для внедрения к 2024 году современной и безопасной цифровой образовательной среды, обеспечивающей формирование ценности к саморазвитию и самообразованию у обучающихся образовательных организаций всех видов и уровней, путем обновления информационно-коммуникационной инфраструктуры, подготовки кадров, создания федеральной цифровой платформы.

Единая информационно-образовательная среда представляется как совокупность платформенных решений, удовлетворяющих любые образовательные запросы и потребности.

Для удовлетворения своих образовательных потребностей в рамках цифровой образовательной среды каждому обучающемуся необходимо овладеть новыми компетенциями. Это, прежде всего, цифровая грамотность (digital fluency), понимаемая как готовность и способность личности применять цифровые технологии уверенно, эффективно, критично и безопасно во всех сферах жизнедеятельности. Согласно ФГОС начального общего и основного общего образования метапредметные результаты освоения основной образовательной программы начального и общего образования должны отражать формирование и развитие компетентности в области использования информационно-коммуникационных технологий. Цифровая грамотность определяется в том числе набором знаний и умений, которые необходимы для безопасного и эффективного использования ресурсов сети Интернет [2].

Интернет повысил доступность для людей разнообразной информации, при этом открыта не только информация чисто развлекательного плана (кино, музыка, игры и т. д.), научного, научно-популярного, учебного и культурного характера, он стал средой для общения, сотрудничества и взаимодействия между людьми без учета географического положения (веб-форумы, блоги, интернет-магазины, социальные сети, электронные платежные системы, мессенджеры), но и несет с собой ряд проблем, требующих контроля и регулирования (это проблемы негативного информационного контента, агрессии и насилия в сети Интернет, распространения вредоносного программного обеспечения, сохранения персональных данных,

мошенничества, сексуального растления несовершеннолетних). В зоне риска оказываются прежде всего дети, которые также являются активными и во многих случаях наиболее продвинутыми пользователями Сети, потребителями разнообразного развлекательного контента, участниками социальных сетей. Современные дети пользуются интернетом дома, в школе на уроках и переменах, в транспорте и любом другом месте, где доступна сеть. Встает вопрос: как оградить ребенка от угроз, которые несет собой интернет? Проблема интернет-безопасности требует комплексного подхода к ее решению и участия в этом процессе родителей, самих учащихся, педагогов, заинтересованных представителей общественности. Это актуализирует потребность в повышении компетентности родителей и педагогических работников по проблеме интернет-безопасности.

Актуальность методических рекомендаций «Интернет безопасность без проблем. Совместный план для родителей, детей и педагогов» заключается в том, что они опираются на уже имеющийся богатый опыт школы безопасности детей «Стоп Угроза». В методических рекомендациях учтены психологические и возрастные особенности, а содержание релевантно интересам и запросам современного общества.

**Цель методических рекомендаций** – оказание методической поддержки образовательным организациям России в организации просвещения обучающихся и их родителей (законных представителей) в области обеспечения интернет-безопасности несовершеннолетних.

**Задачи:**

– познакомить родителей и педагогов с угрозами, которые подстерегают детей в сети Интернет;

– познакомить педагогов с нормативно-правовой базой, основными направлениями работы по проблеме интернет-безопасности, с формами и методами проведения занятий с обучающимися;

– дать информацию об особенностях детей разного возраста, влияющих на содержание работы по проблеме интернет-безопасности;

– предложить образовательным организациям совместный план для педагогов, родителей и детей «Интернет-безопасность без проблем» с указанием примерного перечня мероприятий с участием педагогов, родителей и детей, направленных на ограничение влияния негативных факторов, связанных с использованием сети Интернет, повышение компетентности педагогов, родителей и детей по проблеме интернет-безопасности и создание эффективной системы работы по обеспечению интернет-безопасности обучающихся в образовательной организации;

– представить современные, действенные формы профилактической работы, обеспечивающей формирование ценности к саморазвитию, самообразованию у учащихся;

– дать рекомендации родителям по обеспечению интернет-безопасности несовершеннолетних;

– познакомить педагогов с содержанием тренингов Всероссийской сети частных школ безопасности для детей и родителей «Стоп угроза».

В основе данных методических рекомендаций лежат концепции личностно-ориентированного, деятельностного, инновационно-рефлексивного, системного, аксиологического, практико-ориентированного подходов (Л.И. Божович, Е.В. Бондаревская, А.Н. Леонтьев, С.Л. Рубинштейн, Р.Х. Шакуров, И.С. Якиманская и др.). Научно-практические разработки для педагогов общего образования Л.В. Шаровой. Кроме того, исследования об использовании цифровых технологий в обучении, воспитании и профилактике асоциального поведения периодов, в частности младшего школьного возраста, в их использовании Г.У. Солдатовой, С.В. Чигарьковой, А.А. Дренёвой, С.Н. Илюхина, И.Д. Пермякова и др.

Ожидаемые результаты использования методических рекомендаций:

– образовательные организации актуализируют систему профилактических мероприятий, направленных на защиту детей от видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

– взрослые (педагоги, родители) повысят квалификацию в области обеспечения информационной безопасности детей: актуализируют информацию об основных направлениях работы по проблеме интернет-безопасности, формах и методах проведения занятий с детьми разного возраста, овладеют современными формами профилактической работы, обеспечивающей формирование ценности к саморазвитию, самообразованию у учащихся и будут способны оградить детей от вредной информации в Интернете, путем привития им навыков ответственного и безопасного поведения в информационной среде вне зависимости от уровня владения ИКТ;

– дети (обучающиеся) научатся распознавать манипулятивные техники, используемые при подаче рекламной и иной информации, анализировать степень достоверности информации и подлинность ее источников, овладеют навыками сетевого этикета, смогут избежать интернет-зависимости.

Методические рекомендации распространяются на следующие организации, организующие обучение в очной и очно-заочной:

1. Общеобразовательные организации.
2. Организации дополнительного образования.
3. Организации и индивидуальные предприниматели, осуществляющие образовательную деятельность по программам основного и дошкольного образования.
4. Учреждения для детей-сирот и детей, оставшихся без попечения родителей.

Методические рекомендации имеют следующую структуру:

Раздел «Нормативно-правовая база деятельности образовательных организаций по обеспечению интернет-безопасности обучающихся» направлен на ознакомление педагогических работников с основными положениями нормативно-правовых актов, затрагивающих данную сферу, а также различных аспектах методического обеспечения воспитательной программы образовательной организации по обеспечению информационной и медиабезопасности в образовательном учреждении.

Раздел «Работа педагога над повышением уровня информированности в сфере интернет-безопасности. Типичные проблемы с интернет-безопасностью у учащихся разных возрастов и пути их решения» содержит етодические рекомендации для педагогов начальной школы, среднего и старшего звена, рекомендации для классных руководителей по организации работы с родителями, по организации взаимодействия педагога с заинтересованными в проблеме представителями общественности, специалистами по интернет-безопасности, сотрудниками правоохранительных органов.

В третьем разделе представлен «Совместный план для педагогов, родителей и детей "Интернет-безопасность без проблем"».

В приложении к методическим рекомендациям представлены методы работы с информацией и формирования критического мышления (приложение 1), интерактивные технологии обучения, направленные на формирование у обучающихся знаний, умений и навыков на основе анализа и решения реальной или смоделированной проблемной ситуации в контексте проблемы интернет-безопасности, представленные в виде проектной, кейс и синема технологий (приложения 2, 3, 4), формы и методы работы с обучающимися по проблеме интернет-без-

опасности (приложение 5), варианты анкет мониторинговых исследований по вопросам интернет-безопасности образовательной среды (приложение 6), материалы для подготовки буклетов по правилам поведения в интернет-пространстве для учащихся младшего школьного возраста (приложение 7), методические рекомендации для классных руководителей по проведению классного часа и родительского собрания на тему интернет безопасности детей (приложения 8, 9), примерный план беседы родителей с ребенком на тему безопасности в сети Интернет (приложение 10), списки научной и методической литературы по теме обеспечения интернет-безопасности детей (приложения 11, 12).

# 1. Нормативно-правовая база деятельности образовательных организаций по обеспечению интернет-безопасности обучающихся

Нормативно-правое обеспечение является основой деятельности образовательного учреждения по всем направлениям. В образовательном учреждении должен быть сформирован пакет нормативно-правовой документации федерального, регионального, муниципального и учрежденческого уровней по вопросам информационной безопасности. К таким относятся документы по контентной фильтрации, по обработке персональной информации, положения и регламенты по работе в сети Интернет как педагогических работников, так и школьников, различные положения об организации профилактической работы по медиабезопасности, о формах профилактической работы с детьми и родителями по интернет-безопасности, правила безопасного поведения в сети Интернет. В образовательном учреждении приказами должны быть назначены лица, ответственные за контентную фильтрацию, за работу с персональными данными, за организацией работы школьников в сети Интернет и т. д.

В организационном плане по обеспечению информационной и медиабезопасности в образовательном учреждении должен выполняться ряд мер технико-технологической направленности:

– установка только лицензионного программного обеспечения;

– подключение к системе контентной фильтрации;

– установка антивирусных программ;

– установка и настройка программ-фильтров, брандмауэров.

К организационным внутришкольным мероприятиям относятся:

– разработка и реализация правил интернет-безопасности, с привлечением заинтересованных лиц: директора школы, классных руководителей, преподавателей информационных технологий, самих учащихся и их родителей, поставщиков услуг интернета;

– организация работы детей в интернете по расписанию с ограничением по времени под наблюдением педагогических работников;

– регулярная проверка принимаемых мер в области интернет-безопасности в образовательном учреждении.

Для организации профилактической работы по медиабезопасности с детьми и родителями педагогический работник должен знать проблемы и опасности, которые подстерегают пользователя в сети Интернет, и быть готов дать рекомендации по решению данных проблем.

Для организации профилактических мер в образовательном учреждении необходимо периодически проводить мониторинг, диагностику проблем по интернет-безопасности среди детей и родителей. Данный мониторинг и разъяснительную работу можно проводить с привлечением специалистов школы безопасности «Стоп Угроза» или с помощью иных профессионалов, реализующих проекты по медиабезопасности и способных взять на себя функции школьного модератора, в обязанности которого входит модерация нежелательного содержания в Сети проекта и организация мероприятий с педагогами, родителями и обучающимися по вопросам интернет-безопасности.

В аспекте методического обеспечения воспитательной программы образовательной организации необходимо иметь раздел (программу, модуль), в котором будут включены темы по медиабезопасности, о безопасном поведении в сети Интернет.

В качестве возможного варианта предоставления учащимся соответствующих знаний может быть использована учебная программа, разработанная специалистами «Стоп Угрозы» в рамках проекта по обеспечению информационной безопасности детей «Интернет без про-

блем. Совместный план для педагогов, родителей, детей». Основу программы составляют интерактивные занятия (тренинги для подростков и семинары для родителей), осуществляемые в форме совместной деятельности, наиболее популярные из них: онлайн-квест «Агент безопасности» (7–12 лет), «Защита от похитителя» (5–10 лет), «Безопасный интернет» (9–15 лет), «Девочки в безопасности» (13–17 лет), «Стоп наркотик» (14–17 лет), «Моральное айкидо» (10–17 лет), а также совместные тренинги «родители + дети» и семинары для родителей и школьных педагогов.

Учебный процесс организован тренерами «Стоп Угрозы» таким образом, что в ходе интерактивного занятия меняется взаимодействие преподавателя и обучаемого, родителя и ребенка: активность педагога, родителей (законных представителей) уступает место активности обучаемых (детей), а задачей взрослого становится создание условий для детской инициативы. Для этого на занятиях тренером «Стоп Угрозы» организуются парная и групповая работа, применяются проектные технологии, проводятся сюжетно-ролевые игры, идет работа с документами и различными информационными источниками, выполняются творческие задания.

Вы можете пригласить тренера в школу, лагерь, детский сад, клуб, семью, на предприятие или приехать в центр, реализующий программу «Стоп Угроза».

Заметим, что интерактивные занятия по интернет-безопасности может вести и школьный педагог, психолог, родитель, общественник, при этом важнейшее условие для этого – личный опыт педагогической деятельности и ведения тренинговых занятий.

Рекомендуемая тематика для организации профилактической деятельности:

– нежелательная информация в интернете, как ее избежать;

– проблемы достоверности информации в интернете, как проверить достоверность информации;

– социальные сети: опасности и правила поведения в социальных сетях;

– кибермошенничество, как избежать кибермошенников;

– киберхулиганство, киберзапугивание, правила поведения в опасной виртуальной ситуации;

– вредоносные программы, методы борьбы с ними;

– полезные ссылки, ресурсы, сервисы в интернете.

Тематика проведения различных школьных мероприятий по интернет-безопасности может быть самой разнообразной, например:

– противозаконная, неэтичная и вредоносная информация в интернете, как ее избежать;

– достоверность информации в интернете, проблемы и способы проверки информации на достоверность и полноту;

– этика сетевого общения;

– личная информация: нужна ли она в интернете, как защитить личную информацию в блогах, социальных сетях и пр.;

– социальные сети: как общаться и не попасть в сети мошенников и злоумышленников;

– что такое хакерство: этика и основы;

– интернет-зависимость: угрозы, реальность, проблемы, решения;

– Web-серфинг: как не потерять себя и свое время в интернете;

– как распознать кибермошенничество и не стать жертвой;

– нигерийские письма: предложения в письмах и как не попасться на удочку мошенников;

– что такое киберхулиганство: как не стать жертвой и киберхулиганом;

– как защитить свою почту от спама и не стать спамером;

– компьютерные вирусы и методы борьбы с ними;

– киберпреступления в законодательстве России;

– безопасность в коммерческих интернет-сервисах: интернет-магазины, услуги различных фирм и др.;

– компьютерные игры, как не стать игроманом;

– азартные игры в интернете – поле чудес для..?;

– мобильные угрозы в современном мире;

– как правильно вести себя с киберхулиганами и защититься от нежелательного общения;

– твоя жизнь не игрушка.

Методические рекомендации составлены на основе следующих нормативных документов:

– Федеральный закон «Об образовании в РФ» от 29.12.2012 № 273-ФЗ;

– Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ (с изменениями от 28.07.2012 № 139-ФЗ);

– Письмо Минкомсвязи РФ от 14.08.2012 № 52-165/ВА о применении норм Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

– Письмо Минобрнауки РФ от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»;

– Приказ Минкомсвязи РФ от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию»;

– «Концепция информационной безопасности детей», утверждена распоряжением Правительства РФ от 2.12.2015 № 2471-р;

– Указ Президента РФ от 5.12.2016 № 646 «Об утверждении Доктрины информационной безопасности РФ»;

– Указ Президента РФ от 29.05.2017 № 240 «Об объявлении в РФ Десятилетия детства»;

– методические рекомендации по ограничению в образовательных организациях доступа, обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 16.05.2019).

# 2. Типичные проблемы с интернет-безопасностью у учащихся разных возрастов и пути их решения

Традиционно интернет-безопасность рассматривается как отрасль компьютерной безопасности, связанная с предотвращением атак через сеть интернет, таких как интернет-мошенничество, распространение вредоносного программного обеспечения, кражи персональных данных и т. п.

С педагогической точки зрения интернет-безопасность – это состояние защищенности ребенка, при котором отсутствует риск причинения ему вреда (морального, психологического, физического), связанного с использованием сети Интернет.

Профилактическая работа образовательной организации в области обеспечения информационной безопасности детей основывается на конституционных гарантиях равенства прав и свобод граждан и реализуется в соответствии со следующими принципами:

– признание детей равноправными участниками процесса;

– ответственность педагогических работников, родителей (законных представителей) за соблюдение законных интересов детей в информационной сфере;

– необходимость формирования у детей умения ориентироваться в современной информационной среде;

– воспитание у детей навыков самостоятельного и критического мышления;

– обучение детей медиаграмотности, способности распознавать манипулятивные техники, используемые при подаче рекламной и иной информации, умению анализировать степень достоверности информации и подлинности ее источников, овладение навыками сетевого этикета, которые позволят им избежать интернет-зависимости;

– поддержка творческой инициативы детей в целях их самореализации в информационной среде;

– взаимодействие образовательной организации с различными ведомствами, учреждениями и специалистами при реализации стратегий, планов, программ, мероприятий в части, касающейся обеспечения информационной безопасности детей.

Процесс обеспечения интернет-безопасности подрастающего поколения можно рассматривать как совокупность мероприятий с участием педагогов, родителей и детей, направленных на ограничение влияния негативных факторов, связанных с использованием сети Интернет. В то же время недостаточно ограничительных мер, связанных с регламентацией времени, которое ребенок проводит в Сети, фильтрацией интернет-контента и т. д. Необходимо формировать у детей и подростков навыки безопасного поведения в сети Интернет. Важно научить ребенка безопасно пользоваться сетью с целью плодотворного общения с другими людьми, получения полезных знаний, повышения собственного интеллектуального, культурного и нравственного потенциала [9].

Специфика данной проблемы выдвигает и соответствующие требования к педагогу. Он должен быть активным интернет-пользователем сетевых сервисов (интернет-форумов, чатов, социальных сетей и сетевых сообществ профессиональной направленности), отслеживать новые тенденции развития Сети, обладать навыками критического мышления, уметь анализировать информацию, хорошо ориентироваться в информационном потоке[1].

[1] Приказ для органов власти субъектов Федерации о реализации плана мероприятий Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества на 2018/2019 учебный год..– Текст: электронный // Единый урок: [сайт]. – URL: https://www.единыйурок.рф/index.php/faq/obshchie-voprosy/ekspertnyj-sovet/dokumenty-i-informatsiya-dlya-ispolzovaniya-v-rabote (дата обращения: 24.05.2020).

В профессиональном стандарте «Педагог (педагогическая деятельность в сфере начального общего, основного общего, среднего общего образования; воспитатель; учитель)» среди трудовых функций и необходимых умений выделяется: владение ИКТ-компетентностями (общепользовательская ИКТ-компетентность, общепедагогическая ИКТ-компетентность, предметно-педагогическая ИКТ-компетентность), умение формировать у обучающихся навыки, связанные с информационно-коммуникационными технологиями. Необходимые компетенции педагога будущего: компетенция – знание (набор требуемых знаний по интернет-безопасности); компетенция – навыки, владение методами и средствами выполнения задач; компетенция – способность, предрасположенность, готовность к решению задачи; компетенция – стериотипы поведения, видимые формы действий, поведения, убеждения, реакция на происходящую реальность; и усилия – сознательное приложение в конкретном направлении ментальных и физических ресурсов).

Обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания усилий педагогического коллектива образовательной организации и общественных усилий при определяющей роли семьи. В связи с этим важнейшей задачей является налаживание согласованного взаимодействия между членами педагогического коллектива образовательной организации, психолого-педагогическими экспертными сообществами и семьей как главным институтом социализации и воспитания детей. Только тесное сотрудничество всех участников образовательного процесса позволит построить эффективную информационную среду, максимально безопасную для психического, физического развития и здоровья подрастающего поколения.

Кроме того, совместные усилия всех участников образовательного процесса должны быть направлены на минимизацию рисков десоциализации развития, таких как:

## 2.1. Агрессия и психологическое насилие в сети Интернет (распространение ложных слухов, сплетен о людях, агрессивное поведение и хамство на форумах и в социальных сетях)

Впервые эта проблема привлекла внимание широкой общественности в 2006 году, когда фотографии изуродованного тела Никки Катсурас, погибшей в автокатастрофе (штат Калифорния США), без согласия ее родственников попали в интернет. Неизвестные прислали фотографии отцу девушки с подписью «Девушка-зомби. Эй, папа, я все еще живая!»

## 2.2. Распространение в сети Интернет ложной, недостоверной информации, вводящей пользователей в заблуждение, и информации, которая может нанести вред психическому, нравственному и физическому здоровью несовершеннолетних

Многие пользователи Сети не задумываются над качеством информационных сообщений, поступающих к ним, над их ценностным, нравственным содержанием. Различные источники информации могут формировать не только положительные ценностные установки, но и отрицательные. В итоге современное общество образуют не только информированные, но и введенные в заблуждение ложной информацией люди.

Особенно пагубно негативная информация влияет на незрелую душу ребенка. В Сети возможно распространение информации, побуждающей детей к совершению действий, представляющих угрозу их жизни и здоровью, в том числе к самоубийству; способной вызвать у детей желание употребить наркотические средства, психотропные и одурманивающие вещества, табачные изделия, алкогольную продукцию; оправдывающей допустимость насилия и жестокости по отношению к людям или животным; отрицающей семейные ценности и формирующей неуважение к родителям и другим членам семьи; оправдывающей противоправное поведение; содержащей нецензурную брань, сцены порнографического характера. Система Kaspersky Security Network приводит данные об информации на сайтах с нежелательным контентом, с которой чаще всего сталкиваются дети в Сети: 46,4% – сайты порнографического содержания, 26,4% – оружие, 10,7% – нецензурная лексика, 6,6% – нелегальное программное обеспечение, 5,5% – онлайн-игры, 1,9% – азартные игры, 1,1% – жестокость и насилие, 0,7% – анонимные прокси-серверы, 0,4% – платежные системы, 0,3% – наркотики [5].

## 2.3. Утечка персональных данных и личной информации в интернете

По данным правоохранительных органов, 80% преступников берут информацию в социальных сетях. Личная информация используется для кражи паролей, для совершения таких преступлений, как шантаж, вымогательство, оскорбление, клевета, киднеппинг, кражи.

## 2.4. Мошенничество

В сети Интернет распространены такие виды мошенничества, как сайты-подделки, распространяющие вирусы и навязывающие платные услуги; мошенничество с использованием банковских карт; фишинговые сообщения, отправленные от имени администраторов банковских или других платежных систем, призывающие пользователей пройти по фальшивой ссылке на сайт, ставящий под угрозу конфиденциальные данные пользователя.

## 2.5. Сексуальное растление несовершеннолетних взрослыми в сети Интернет

Одной из современных проблем интернета являются вовлечение несовершеннолетних в общение с взрослыми, носящее деструктивный характер, различные виды сексуального насилия. Один из видов преступного поведения взрослых – кибергруминг, это действия, направленные на растление детей в интернете через все возможные каналы коммуникации (чаты, мессенджеры, социальные сети и т. д.). Преступники используют эти ресурсы для установления близких отношений со своими жертвами. После вхождения в доверие грумер (преступник) вынуждает жертву отправить фото сексуального или порнографического характера.

## 2.6. Кибербуллинг

Буллинг – систематическое, регулярно повторяющееся насилие (травля) в детской, подростковой среде сегодня переместился в интернет. Травля стала происходить в социальных сетях, на форумах, в письмах, в мессенджерах, в чатах, в онлайн-играх. Буллеры создают страницы, посвященные издевательствам над жертвой травли, постят карикатуры, публикуют унизительные фотографии или видео, распространяют о жертвах слухи, отправляют личные сообщения с оскорблениями и угрозами, публикуют сведения о жертве вопреки ее воле, шантажируют, разглашают личную информацию и т. д.

Виды кибербуллинга:

– **Исключение** – вариант бойкота, когда ребенка исключают из игры или сообщества, или из беседы, чатов, общих обсуждений.

– **Домогательство** – если ребенок регулярно получает оскорбительные сообщения от одного человека, нескольких или от имени группы, иногда бывает так, что такие сообщения приходят каждый день.

– **Аутинг** – когда кто-то намеренно выкладывает в общий доступ или передает кому-то личную информацию ребенка, переписку, фотографии.

– **Киберсталкинг** – преследование (например, кто-то может угрожать или шантажировать ребенка и при этом требовать личной встречи, или чтобы жертва передала ему деньги, или что-то сделала под любой угрозой).

– **Фрейпинг** – если кто-то взломал страницу ребенка и что-то постит от его имени, или кому-то пишет.

– **Поддельные профили** – кто-то пишет ребенку, используя липовую страницу, (например, используя липовую страницу могут рассказывать что-то личное какой-то подруге, а потом узнать, что это не она, а какой-то ваш враг); есть еще такой вариант подделки, когда кто-то крадет ваши фото и всю личную информацию и создает липовый профиль от вашего имени (или несколько), чтобы вас каким-то образом унизить (например, он может вступить в переписку с кем-то, кто вам дорог, и испортить отношения с этим человеком или писать как бы от вашего имени, давать объявления, вступать в группы, переписываться с кем-то из ваших друзей).

# Конец ознакомительного фрагмента.