Муниципальное казённое общеобразовательное учреждение

«Талицкая средняя общеобразовательная школа №1»

 ***«Кибербуллинг и онлайн преступления»***

Учебно-исследовательская работа по обществознанию

проектант:

учащаяся 10 «Б» класса

Шимолиной Алёны Денисовны

Руководитель проекта:

Бабакина Елизавета Игоревна

учитель истории и обществознания

 Талица 2025г.

# Содержание

[Содержание 2](#_Toc195047289)

[Введение 3](#_Toc195047290)

[1.1 Определение и виды кибербуллинга 4](#_Toc195047291)

[1.2 Психологические факторы, способствующие кибербуллингу 5](#_Toc195047292)

[1.3 Социальные и культурные аспекты кибербуллинга 7](#_Toc195047293)

[1.4 Причины возникновения кибербуллинга среди молодежи 8](#_Toc195047294)

[1.5 Последствия кибербуллинга для жертв 10](#_Toc195047295)

[1.6 Долгосрочные эффекты кибербуллинга на общество 12](#_Toc195047296)

[2.1 Разновидности онлайн преступлений: мошенничество и кража личных данных 14](#_Toc195047297)

[2.2 Распространение вредоносного контента и его последствия 15](#_Toc195047298)

[2.3 Сравнительный анализ кибербуллинга и других форм онлайн преступлений 16](#_Toc195047299)

[2.4 Законодательные инициативы и их эффективность 18](#_Toc195047300)

[2.5 Роль образовательных программ в профилактике кибербуллинга 19](#_Toc195047301)

[2.6 Технологические решения для защиты пользователей 20](#_Toc195047302)

[2.7 Личные меры безопасности для пользователей 22](#_Toc195047303)

[2.8 Создание безопасной онлайн-среды для молодежи 22](#_Toc195047304)

[2.9 Рекомендации для родителей и педагогов по предотвращению кибербуллинга 23](#_Toc195047305)

[Заключение 25](#_Toc195047306)

[Список литературы 26](#_Toc195047307)

# Введение

**Актуальность темы:** в последние годы в социальных сетях наблюдается значительный рост использования интернета и мобильных устройств среди детей и подростков. Это создает новые возможности для взаимодействия, но также и новые риски, включая кибербуллинг и другие формы онлайн-преступлений

**Проблема:** как технологии способствуют распространению кибербуллинга и онлайн-преступлений среди детей?

**Цель:** исследовать влияние технологий на преступность среди детей, в частности на кибербуллинг и преступления в интернете.

**Задачи:**

1. Исследовать и собрать данные о случаях кибербуллинга и других онлайн-преступлений среди детей и подростков.

2. Провести исследование причин, способствующих кибербуллингу и другим формам онлайн-преступлений.

3. Изучить последствия кибербуллинга для жертв, включая психологические, эмоциональные и социальные аспекты.

4. Изучить существующие методы профилактики кибербуллинга и онлайн-преступлений.

**Объект** - подростки и дети.

**Предмет -** люди

**Гипотеза:** "Если доступ детей к цифровым технологиям и социальным сетям увеличивается, то это приводит к росту случаев кибербуллинга и онлайн-преступлений среди молодежи."

**Методы исследования:**

1.  Анализ случаев

2. Теоретический анализ

3. Систематизация знаний

**Список литературы**

Глава 1. Психология кибербуллинга и его проявления

1.1 Определение и виды кибербуллинга

Кибербуллинг представляет собой форму агрессивного поведения, осуществляемого через цифровые технологии, такие как социальные сети, мессенджеры, форумы и другие онлайн-платформы. Это явление включает намеренное причинение вреда другому человеку посредством оскорблений, угроз, распространения ложной информации или других действий, направленных на унижение и дискредитацию жертвы. Ключевой характеристикой кибербуллинга является его постоянство и систематичность, что усиливает психологическое воздействие на пострадавших. В статье рассматриваются криминалистические аспекты кибербуллинга как формы деструктивного поведения в сети Интернет, а также его психологические особенности и разнообразные формы проявления [4].

Кибербуллинг проявляется в различных формах, каждая из которых имеет свои особенности и последствия. Наиболее распространенные из них включают оскорбления и унижения в комментариях, распространение ложной информации или слухов, создание фальшивых профилей для дискредитации других, а также прямые угрозы через сообщения. Эти действия могут быть направлены как на отдельных пользователей, так и на группы людей, что усложняет проблему предотвращения кибербуллинга. Все эти формы могут быть особенно опасными для молодежи, так как они вызывают чувство изоляции, сильного давления и низкую самооценку [6].

Одним из ключевых отличий кибербуллинга от традиционного буллинга является использование цифровых технологий в качестве основного инструмента агрессии. Это позволяет агрессорам оставаться анонимными, что значительно усложняет их идентификацию и привлечение к ответственности. В отличие от традиционного буллинга, который ограничен физическим пространством, кибербуллинг не имеет пространственных и временных рамок. Такое отсутствие границ делает его воздействие на жертву постоянным и всепроникающим. Исследования показывают, что «более агрессивные и невротичные, менее эмпатичные и толерантные подростки чаще выступают в роли агрессоров не только в условиях традиционного буллинга, но и в онлайне» [14]. Это подчеркивает важность комплексного подхода к пониманию причин кибербуллинга, учитывающего как личностные характеристики агрессоров, так и особенности онлайн-среды.

Примеры кибербуллинга включают случаи, когда подростки подвергаются оскорблениям в социальных сетях, их фотографии используются без разрешения для создания компрометирующего контента, а ложные слухи о них распространяются среди сверстников. Кибербуллинг в подростковой среде представляет собой актуальную проблему современного общества, где прослеживается триада: агрессор, наблюдатель и жертва [2]. Исследование Pew Research Center показывает, что около 59% подростков в США сталкивались с кибербуллингом, что подчеркивает значимость этой проблемы. В 2019 году в Великобритании было зарегистрировано более 10 000 случаев кибербуллинга среди подростков, что также демонстрирует масштабы этого явления.

1.2 Психологические факторы, способствующие кибербуллингу

Агрессоры, участвующие в кибербуллинге, часто обладают определенными личностными характеристиками, способствующими их поведению. Исследования показывают, что около 40% таких людей имеют низкую самооценку, что побуждает их к агрессивным действиям в отношении других. Это может быть связано с желанием компенсировать собственные недостатки через доминирование над окружающими. Вместе с тем, агрессоры могут проявлять склонность к нарциссизму и недостаток эмпатии, что делает их менее чувствительными к страданиям жертв. Анализируя работы российских авторов, можно отметить, что зависть является скрытым и зачастую неосознаваемым чувством, которое может приводить к кибербуллингу [1].

Жертвы кибербуллинга, как правило, имеют свои уникальные психологические особенности, которые могут увеличивать их уязвимость. Согласно исследованиям, такие люди в два раза чаще страдают от депрессии и тревожных расстройств, чем те, кто не сталкивался с этим явлением. Эти состояния могут быть как причиной, так и следствием кибербуллинга, создавая порочный круг, из которого жертве сложно выбраться. Понимание этих особенностей помогает в разработке профилактических мер и программ поддержки.

Анонимность, предлагаемая интернетом, существенно способствует распространению кибербуллинга, снижая уровень самоконтроля у пользователей и провоцируя более агрессивное поведение. Осознавая свою защищенность от идентификации, люди нередко выражают эмоции и мысли, игнорируя социальные нормы. Это создает благоприятную среду для агрессоров, позволяя им уклоняться от ответственности за свои действия. В этом контексте важно учитывать, что «лукизм – критика человека за внешность, не попадающую, по мнению комментатора, под общепринятые стандарты красоты» [13]. Подобные явления становятся особенно распространенными в интернет-пространстве, где анонимность усиливает негативные проявления, такие как агрессия и предвзятость.

Одной из причин распространенности кибербуллинга является отсутствие реальных последствий для агрессоров. В отличие от традиционного буллинга, где агрессор может столкнуться с немедленной реакцией окружающих, в интернете действия часто остаются безнаказанными, что создает иллюзию вседозволенности и поощряет агрессивное поведение. Акиньшина, Пирязева и Анцева отмечают, что «можем выделить следующие причины развития кибербуллинга: 1. Стремление к превосходству в негативном ключе – чувство, присущее каждому индивиду, от которого невозможно избавиться» [6]. Поэтому для борьбы с этим явлением важно разрабатывать меры, усиливающие ответственность за действия в сети.

1.3 Социальные и культурные аспекты кибербуллинга

Социальные нормы играют ключевую роль в формировании поведения в интернете. Они определяют, какие действия считаются приемлемыми, а какие — нет. В контексте кибербуллинга это означает, что общества, где агрессивное поведение в сети осуждается, сталкиваются с меньшей распространенностью этого явления. Например, в Австралии принятие закона Enhancing Online Safety Act подчеркивает важность установления четких норм и стандартов поведения в интернете, что способствует снижению уровня онлайн-агрессии.

Культурные особенности оказывают значительное влияние на восприятие и проявление кибербуллинга. Исследования показывают, что в обществах с высоким уровнем коллективизма, таких как Япония или Южная Корея, уровень кибербуллинга ниже, чем в индивидуалистических культурах, например, в США. Это объясняется тем, что коллективистские культуры акцентируют внимание на гармонии в межличностных отношениях и социальной ответственности, что способствует меньшей агрессии в сети. Вместе с тем, «Интернет-пространство явилось ярким феноменом в современной жизни мирового сообщества, оно затрагивает все сферы общества: экономическую, социальную, политическую и духовную» [17]. Таким образом, культурные контексты формируют не только поведение пользователей в сети, но и общее восприятие кибербуллинга.

Групповая динамика играет важную роль в распространении кибербуллинга. Когда агрессивное поведение становится нормой в определенной группе, это может побуждать её членов действовать аналогично. Социальные сети часто создают условия для формирования таких групп, где участники поддерживают и усиливают агрессивные действия друг друга. Это явление также известно как эффект quot;зараженияquot; агрессией, который усиливается благодаря анонимности и отсутствию реальных последствий.

Медиа и поп-культура оказывают значительное влияние на восприятие кибербуллинга. Фильмы, сериалы и социальные сети могут как способствовать нормализации агрессивного поведения, так и служить инструментом для осуждения подобных действий. Например, компания Facebook внедрила инструменты для автоматического выявления оскорбительных комментариев, что стало важным шагом в снижении уровня кибербуллинга на платформе. Это подчеркивает необходимость ответственного подхода к созданию и распространению контента.

1.4 Причины возникновения кибербуллинга среди молодежи

Социальные факторы оказывают значительное влияние на возникновение кибербуллинга среди молодежи. В современном обществе, где социальные сети и онлайн-платформы стали неотъемлемой частью повседневной жизни, подростки часто сталкиваются с давлением со стороны сверстников. Исследование Pew Research Center показывает, что 59% подростков в США сталкивались с кибербуллингом. Это связано с тем, что социальные сети создают среду, в которой легко распространять агрессию и унижение. Анонимность и отсутствие непосредственного контакта снижают уровень эмпатии, что делает кибербуллинг более распространенным явлением. Бочавер и Хломов отмечают, что «в ходе нашего анкетирования мы выяснили, что в молодёжной среде проблема кибербуллинга остается актуальной. В основном подвержены интернет-травле подростки» [5].

Психологические причины играют ключевую роль в формировании кибербуллинга. Низкая самооценка, потребность в доминировании и стремление утвердить свое превосходство над другими часто становятся мотивами агрессивного поведения в интернете. Хирина отмечает, что «проблема травли и преследования в среде старшеклассников всегда была и остается актуальной. Старшеклассник еще сохраняет в себе черты подросткового возраста и формирующиеся признаки юношества» [16]. Важно также учитывать, что черты личности, такие как импульсивность и склонность к агрессии, нередко проявляются в онлайн-пространстве, где отсутствуют непосредственные последствия для агрессора. Это создает условия, при которых подростки могут использовать кибербуллинг как способ самоутверждения или снятия внутреннего напряжения.

Технологии играют двойственную роль в вопросе кибербуллинга. С одной стороны, они предоставляют уникальные возможности для общения и самовыражения, с другой — создают платформу для агрессии и травли. В 2020 году в мире насчитывалось более 4,5 миллиарда пользователей интернета, что значительно увеличило доступность ресурсов для кибербуллинга. Развитие таких технологий, как анонимные чаты и временные сообщения, усложняет выявление и предотвращение случаев травли в сети, что делает эту проблему более актуальной. Белковец [3] подчеркивает, что «в современном мире в связи с развитием информационных технологий многие психологические явления приобретают новое звучание. В частности, это касается феномена агрессии среди подростков, который приобрел новую форму – кибербуллинг».

Семейная среда оказывает значительное влияние на поведение подростков в интернете. Семейные конфликты, недостаток внимания и контроля со стороны родителей часто приводят к тому, что дети выражают свою агрессию в онлайн-пространстве. Подростки, не получающие поддержки в семье, могут искать способы привлечь внимание или справиться с эмоциями через агрессивное поведение в интернете. Это подчеркивает важность вовлеченности родителей в жизнь своих детей и их активного участия в формировании здоровых моделей поведения.

Культурные и образовательные аспекты играют ключевую роль в предотвращении кибербуллинга. В странах с высоким уровнем цифровой грамотности наблюдается меньший уровень кибербуллинга, что связано с образовательными программами, направленными на развитие эмпатии и осознания последствий онлайн-агрессии. Школы и образовательные учреждения выступают важными площадками для информирования молодежи о вреде кибербуллинга и методах его предотвращения. В этом контексте исследование кибербуллинга среди школьников и студентов раскрывает понятия, сущность, причины и виды травли в Интернете [2]. Развитие культуры уважения и ответственности в онлайн-пространстве представляет собой важный шаг к снижению уровня кибербуллинга среди молодежи.

1.5 **Последствия кибербуллинга для жертв**

Кибербуллинг оказывает значительное влияние на психологическое состояние жертв. Исследование 2021 года показало, что жертвы кибербуллинга имеют в 2,3 раза больше шансов страдать от депрессии. Постоянное воздействие агрессивных сообщений, угроз и унижений в онлайн-пространстве приводит к повышению уровня тревожности и стресса. Жертвы могут ощущать изоляцию, беспомощность и потерянность, что усугубляет их эмоциональное состояние и может вызвать долгосрочные психологические проблемы.Основным мотивом агрессоров в кибербуллинге является выражение личной неприязни и зависти, а также стремление повысить свой авторитет в компании друзей. Как отмечает Белковец [3], это подчеркивает сложность явления, где личные чувства агрессоров и социальные факторы переплетаются, усиливая негативное воздействие на психику жертв.

Влияние кибербуллинга на физическое здоровье жертв проявляется через психосоматические симптомы. У жертв часто наблюдаются проблемы со сном, головные боли и расстройства пищеварения, вызванные хроническим стрессом. Постоянное напряжение может оказывать негативное воздействие на иммунную систему, делая жертв более уязвимыми к заболеваниям. Таким образом, кибербуллинг воздействует не только на психическое, но и на физическое здоровье пострадавших.

Одним из значительных последствий кибербуллинга является социальная изоляция. Жертвы часто избегают социальных контактов из-за страха столкнуться с насмешками или осуждением, что приводит к снижению их социальной активности и ухудшению коммуникационных навыков. Исследования показывают, что «целями агрессора является ухудшение эмоционального состояния жертвы, а также разрушение ее социальных отношений» [10]. Усиление социальной изоляции в свою очередь способствует углублению чувства одиночества и беспомощности, что еще больше ухудшает их эмоциональное состояние.

Кибербуллинг оказывает негативное влияние на образовательный процесс и профессиональную деятельность жертв. Согласно отчету ЮНИСЕФ, дети, подвергшиеся кибербуллингу, в три раза чаще пропускают занятия в школе. Постоянное стрессовое состояние затрудняет сосредоточение на обучении и снижает успеваемость. Важно отметить, что «52% подростков сталкиваются с травлей в школах. 38% студентов подвергались издевательствам в высших учебных заведениях. И только 10% взрослых подверглись буллингу и кибербуллингу» [11]. В профессиональной сфере жертвы испытывают трудности с выполнением своих обязанностей, что связано со снижением мотивации и уверенности в себе.

Одним из самых серьёзных последствий кибербуллинга является повышенный риск суицидального поведения у жертв. Постоянное давление и унижения в онлайн-пространстве могут привести к тому, что жертвы начинают видеть единственный выход в прекращении своей жизни. Это подчеркивает необходимость срочной поддержки и вмешательства для предотвращения трагических исходов.

1.6 Долгосрочные эффекты кибербуллинга на общество

Кибербуллинг оказывает значительное влияние на уровень общественного доверия. Исследование Pew Research Center показывает, что более 60% пользователей интернета сталкивались с онлайн-агрессией, что приводит к снижению уверенности в безопасности цифровых платформ. В результате люди начинают избегать общения в интернете, опасаясь стать жертвами нападок. Это подрывает основу доверительных отношений в обществе и формирует замкнутый круг недоверия, затрудняющий конструктивное взаимодействие в онлайн-пространстве.Согласно исследованию кибербуллинга, мальчики более подвержены этому явлению, в то время как девочки демонстрируют большую зависимость от интернета [7].

Экономические последствия кибербуллинга проявляются в различных аспектах. Прямыми результатами этой проблемы являются затраты на лечение жертв, снижение производительности труда и потеря квалифицированных работников. Кибербуллинг представляет собой серьезную угрозу, негативно влияющую на молодежь и общество, и его последствия могут быть крайне разнообразными и долгосрочными [6]. В связи с этим организации и компании вынуждены внедрять программы для предотвращения буллинга, что требует значительных финансовых вложений. Все эти факторы в совокупности оказывают негативное влияние на экономику.

Кибербуллинг в образовательной среде оказывает разрушительное воздействие на процесс обучения. Данные Национального центра образовательной статистики США показывают, что учащиеся, подвергшиеся кибербуллингу, демонстрируют снижение успеваемости и увеличение числа прогулов. Это негативно сказывается как на образовательной системе в целом, так и на культурной атмосфере, формируя среду страха и недоверия. Проект, направленный на повышение компьютерной грамотности и компетентности учащихся в вопросах кибербуллинга, способствует воспитанию культуры поведения в интернет-пространстве [5].

Кибербуллинг стал причиной изменений в законодательстве и социальной политике. В 2019 году в Европейском Союзе были приняты законы, направленные на защиту пользователей от онлайн-агрессии. Эти меры свидетельствуют о необходимости адаптации нормативной базы к новым вызовам цифровой эпохи. Законодательные изменения помогают формировать более безопасную среду в интернете, способствуя снижению уровня кибербуллинга.

Глава 2. Анализ онлайн преступлений

2.1 Разновидности онлайн преступлений: мошенничество и кража личных данных

Мошенничество в интернете представляет собой умышленные действия с целью обмана пользователей для получения финансовой или иной выгоды. Это явление охватывает широкий спектр методов, включая поддельные сайты, фишинговые письма и ложные предложения услуг. Основная цель интернет-мошенников заключается в извлечении выгоды за счет доверчивости и недостатка знаний у пользователей.

Существуют различные виды интернет-мошенничества, включая фишинг, мошенничество с использованием поддельных интернет-магазинов, а также схемы с обещанием быстрого обогащения. Например, фишинг включает отправку поддельных писем или сообщений, которые побуждают пользователей раскрывать свои личные данные. Мошенничество с поддельными интернет-магазинами предполагает создание сайтов, предлагающих товары или услуги, которые на самом деле не существуют.

Кража личных данных является одним из наиболее распространенных видов киберпреступлений. Основной целью злоумышленников является использование украденной информации для финансовых махинаций, например, для доступа к банковским счетам. Существуют различные способы кражи данных, включая использование вредоносного программного обеспечения, взломы баз данных и поддельные запросы на ввод данных.

Жертвы интернет-мошенничества и кражи данных сталкиваются с серьезными последствиями, включая финансовые потери, утрату конфиденциальности и психологический стресс. Например, согласно исследованию компании IBM, утечка данных обходится компаниям в среднем в 4,45 миллиона долларов, что подчеркивает масштаб проблемы.

Технологии играют ключевую роль в предотвращении и борьбе с интернет-преступлениями. Использование систем искусственного интеллекта и машинного обучения помогает выявлять подозрительные действия и предотвращать атаки. Например, современные антивирусные программы и системы защиты данных способны обнаруживать и блокировать вредоносное программное обеспечение, что значительно снижает риски для пользователей.

2.2 Распространение вредоносного контента и его последствия

Вредоносный контент включает материалы, созданные или распространяемые с целью причинения вреда пользователям. К основным видам такого контента относятся дезинформация, фишинговые сообщения, вредоносные программы, такие как вирусы и трояны, а также материалы, направленные на разжигание ненависти или дискриминации. Согласно отчету компании Symantec, в 2021 году было зафиксировано более 5,5 миллиарда попыток распространения фишинговых писем, что свидетельствует о масштабах проблемы.Среди форм шейминга, таких как ланч-шейминг и кофе-шейминг, наблюдается публичное унижение и критика людей по различным причинам [17]. Эти явления также способствуют распространению вредоносного контента, создавая негативную атмосферу в обществе.

Механизмы распространения вредоносного контента разнообразны и включают использование электронной почты, социальных сетей, мессенджеров и других онлайн-платформ. Злоумышленники активно применяют спам-рассылки, поддельные сайты и зараженные файлы для распространения вредоносного контента. Например, Facebook и YouTube являются основными платформами, где пользователи чаще всего сталкиваются с дезинформацией, как указывает исследование Oxford Internet Institute.

Вредоносный контент оказывает значительное влияние на пользователей, включая финансовые потери, утрату конфиденциальной информации и психологический стресс. Вредоносные программы, такие как трояны и вирусы, составляют более 50% всех кибератак, согласно данным Kaspersky Lab, что свидетельствует о серьезных угрозах для кибербезопасности пользователей.

Социальные платформы играют ключевую роль как в распространении, так и в контроле за вредоносным контентом. Они предоставляют злоумышленникам возможности для распространения вредоносных материалов, но также разрабатывают меры для их блокировки. Например, Google в 2020 году заблокировал более 2,7 миллиарда вредоносных объявлений, стремясь защитить пользователей от мошенничества и фишинга.

Для противодействия распространению вредоносного контента необходимо применять комплексные меры, включающие использование современных технологий, просвещение пользователей и международное сотрудничество. Согласно исследованию Pew Research Center, около 41% пользователей интернета сталкивались с различными формами вредоносного контента, что подчеркивает необходимость активных действий в этом направлении.

2.3 Сравнительный анализ кибербуллинга и других форм онлайн преступлений

Кибербуллинг представляет собой форму агрессивного поведения, направленного на унижение, запугивание или оскорбление человека через интернет. Это может включать распространение ложной информации, оскорбительные комментарии или угрозы. Среди форм кибербуллинга выделяются такие проявления, как принуждение жертвы к действиям, социальная изоляция и запугивание, а также использование и распространение персональной информации жертвы [4]. В отличие от кибербуллинга, другие формы онлайн-преступлений, такие как мошенничество, кража данных и распространение вредоносного контента, имеют целью извлечение материальной или иной выгоды за счет жертв. Несмотря на различия в методах и целях, все эти преступления используют цифровую среду для реализации своих намерений.

Общей чертой кибербуллинга и других форм онлайн-преступлений является использование цифровых технологий для достижения своих целей. Халфина отмечает, что «развитие инфокоммуникационных технологий привело к распространению кибербуллинга – агрессивного, умышленного действия, совершаемого группой лиц или одним лицом с использованием электронных форм контакта» [8]. В обоих случаях злоумышленники используют анонимность и широкий доступ к аудитории, предоставляемый интернетом. При этом многие онлайн-преступления, такие как мошенничество, могут наносить значительный психологический вред жертвам, вызывая у них стресс и тревогу.

Основное различие между кибербуллингом и другими формами онлайн-преступлений заключается в их целях. Кибербуллинг, как правило, направлен на психологическое воздействие и унижение жертвы, тогда как такие преступления, как мошенничество или кража данных, стремятся к получению материальной выгоды. При этом кибербуллинг чаще всего проявляется в социальных сетях, в то время как другие виды преступлений могут быть связаны с финансовыми платформами или электронной почтой.Важно отметить, что «нередко через Интернет формируются криминальные группировки, особенно те, которые имеют международный характер. Их коммуникация, планирование, как и совершение уголовного преступления, было бы невозможно без обращения к технологии Интернета» [10]. Это подчеркивает, что хотя кибербуллинг и другие онлайн-преступления могут пересекаться в контексте использования технологий, их цели и методы остаются различными.

Понимание сходств и различий между кибербуллингом и другими формами онлайн преступлений играет ключевую роль в разработке эффективных мер противодействия. Например, для борьбы с кибербуллингом важно учитывать его психологические аспекты, тогда как для предотвращения мошенничества необходимы технические меры защиты. Комплексный подход, учитывающий особенности различных угроз, позволяет создать более эффективные стратегии защиты пользователей.

2.4 Законодательные инициативы и их эффективность

Законодательные инициативы играют ключевую роль в борьбе с кибербуллингом и другими формами онлайн-преступности. В последние годы многие страны осознали необходимость создания правовой базы для регулирования поведения в интернете. Согласно отчету ООН, более 70% стран приняли законы, направленные на противодействие киберпреступлениям. Эти законы охватывают защиту личных данных, борьбу с кибербуллингом и пресечение распространения вредоносного контента. В некоторых государствах, например, предусмотрено уголовное наказание за онлайн-преследование или угрозы, что служит важным сдерживающим фактором для потенциальных нарушителей. При этом Буткевич, Петрожицкая и Гончарова отмечают, что «противодействие преступности в сфере информационно-коммуникационных технологий в настоящее время заключается в совершенствовании и развитии существующей системы борьбы с киберпреступностью» [12].

Несмотря на наличие законодательства, эффективность его применения в борьбе с кибербуллингом и онлайн-преступлениями остается под вопросом. В 2021 году в США было зарегистрировано более 300 тысяч случаев киберпреступлений, несмотря на строгие законы. Это свидетельствует о том, что одних только правовых норм недостаточно для полного искоренения проблемы. Часто жертвы не обращаются за помощью из-за страха или недоверия к правоохранительным органам. Однако, там, где законы активно применяются, наблюдается снижение числа преступлений, что подчеркивает необходимость усиления их исполнения.

Основными недостатками существующего законодательства являются его ограниченность и сложность применения. Согласно исследованию ESET, только 40% пользователей считают законы достаточными для защиты в интернете. Это связано с быстрым развитием технологий, из-за чего правовые нормы часто не успевают адаптироваться к новым вызовам. Кроме того, международная природа интернета создает сложности в координации между странами. Многие преступники пользуются юрисдикционными пробелами, чтобы избежать наказания. Таким образом, необходимо совершенствовать законодательные механизмы и усиливать международное сотрудничество для повышения их эффективности.

2.5 Роль образовательных программ в профилактике кибербуллинга

Образовательные программы играют ключевую роль в профилактике кибербуллинга, так как они направлены на повышение осведомленности и развитие навыков безопасного поведения в интернете. Исследование Pew Research Center показывает, что 59% подростков в США сталкивались с кибербуллингом, что подтверждает необходимость информирования молодежи о рисках и способах предотвращения подобных ситуаций. Эти программы формируют у школьников и студентов осознание ответственности за свои действия в сети, обучая их распознавать и реагировать на проявления кибербуллинга.При этом важно учитывать, что, как указывает Егорова, «объект исследования - подросток, предмет - проявление кибербуллинга в подростковом возрасте». Исследование демонстрирует, что мальчики чаще подвергаются кибербуллингу в интернете, тогда как девочки проявляют большую зависимость от интернета. Это подчеркивает необходимость комплексного подхода к образовательным программам, учитывающим гендерные различия в восприятии и переживании кибербуллинга.

Примеры успешных образовательных инициатив подтверждают их значимость. В частности, в Австралии программа eSmart Schools, направленная на обучение школьников и педагогов основам цифровой безопасности, продемонстрировала снижение случаев кибербуллинга на 30% в школах, внедривших эту программу. Данный случай иллюстрирует, что системный подход к обучению может существенно уменьшить масштабы проблемы и создать безопасную онлайн-среду для детей и подростков. Проблема кибербуллинга особенно серьезна для нашей страны, которая находится среди лидеров по травле в сети в мире, преимущественно за счет детей школьного возраста [10].

Внедрение образовательных программ, обладая значительными преимуществами, сталкивается с рядом проблем. В 2020 году в России было зарегистрировано более 20 000 обращений в службу помощи quot;Дети Онлайнquot;, что указывает на недостаточность существующих инициатив. Основные препятствия включают нехватку ресурсов, недостаточную подготовку педагогов и низкий уровень осведомленности родителей. Для эффективного решения таких проблем, как кибербуллинг, важно проводить обучение как для родителей, так и для учителей. «Предлагается использовать различные игры, бюллетени с советами, проводить форумы, уроки, создавать веб-сайты о кибер-травле и предоставлять эту информацию детям, родителям, учителям» [12]. Перспективы внедрения таких программ выглядят многообещающими, особенно с учетом растущего интереса к цифровой грамотности и поддержки со стороны государственных и общественных организаций.

2.6 Технологические решения для защиты пользователей

Технологические инструменты играют важную роль в борьбе с кибербуллингом, предоставляя возможности для автоматического выявления и блокировки нежелательного контента. Современные платформы социальных сетей, такие как Facebook и Instagram, активно используют системы искусственного интеллекта для анализа пользовательского контента и выявления оскорбительных сообщений, комментариев и изображений. Эти алгоритмы позволяют оперативно удалять вредоносный контент, что способствует созданию безопасной среды для пользователей. Однако эффективность таких систем зависит от их способности адаптироваться к новым формам кибербуллинга и учитывать культурные особенности общения.

Системы защиты от кражи данных и мошенничества являются важным компонентом обеспечения безопасности в интернете. Современные технологии, такие как двухфакторная аутентификация и шифрование данных, предоставляют пользователям надежные инструменты для защиты их личной информации. Однако, несмотря на развитие таких технологий, в 2021 году более 330 миллионов человек по всему миру стали жертвами киберпреступлений, что указывает на необходимость дальнейшего совершенствования систем безопасности. Компании, предоставляющие онлайн-услуги, должны внедрять более сложные механизмы защиты, чтобы минимизировать риски утечек данных и финансовых потерь.

Искусственный интеллект (ИИ) играет ключевую роль в современных системах обеспечения безопасности пользователей в интернете. По данным исследования IBM, 60% компаний уже используют технологии ИИ для предотвращения кибератак. Такие системы способны анализировать огромные объемы данных в реальном времени, выявлять подозрительную активность и предлагать решения для предотвращения угроз. Однако необходимо учитывать, что ИИ требует постоянного обновления и адаптации к новым видам угроз, чтобы оставаться эффективным инструментом в борьбе с киберпреступлениями.

2.7 Личные меры безопасности для пользователей

Основные личные меры безопасности в интернете включают использование сложных и уникальных паролей для каждого онлайн-аккаунта. Согласно исследованию компании Verizon, около 81% утечек данных происходит из-за слабых или украденных паролей. Это подчеркивает важность создания надежных паролей, которые должны содержать комбинацию букв, цифр и специальных символов. Кроме того, рекомендуется использовать двухфакторную аутентификацию, которая добавляет дополнительный уровень защиты. Пользователи также должны быть осторожны при вводе своих данных на подозрительных сайтах и избегать использования общедоступных сетей Wi-Fi без защиты.

Безопасное поведение в интернете предполагает осведомленность о потенциальных угрозах и следование рекомендациям для их предотвращения. Например, пользователи должны избегать открытия подозрительных ссылок и вложений, которые могут содержать вредоносное ПО. По данным Центра кибербезопасности Великобритании, 23,2 миллиона аккаунтов по всему миру используют пароль #039;123456#039;, что делает их уязвимыми для взлома. Поэтому пользователи должны регулярно обновлять свои пароли и использовать менеджеры паролей для их безопасного хранения. Также важно быть осторожным при обмене личной информацией в социальных сетях, чтобы избежать её использования злоумышленниками.

2.8 Создание безопасной онлайн-среды для молодежи

Образовательные инициативы играют ключевую роль в создании безопасной онлайн-среды для молодежи. Важно, чтобы подростки были осведомлены о рисках, с которыми они могут столкнуться в интернете, и знали, как правильно реагировать на угрозы. Согласно исследованию Pew Research Center 2018 года, 59% подростков в США сталкивались с кибербуллингом, что подчеркивает необходимость образовательных программ. Такие программы могут включать в себя уроки и семинары, направленные на повышение цифровой грамотности, обучение безопасному поведению в интернете и развитие навыков критического мышления. Поддержка со стороны школ и образовательных учреждений является важным аспектом в реализации таких инициатив.

Технологии также играют важную роль в создании безопасной онлайн-среды для молодежи. Современные инструменты, такие как системы родительского контроля, фильтры контента и специальные приложения, способствуют защите детей от нежелательной информации и онлайн-угроз. Например, в 2021 году компания Google внедрила функцию quot;Family Linkquot;, которая позволяет родителям контролировать активность детей в интернете, что значительно улучшает безопасность. Кроме того, использование технологий для мониторинга и анализа поведения в интернете может помочь выявлять и предотвращать случаи кибербуллинга. Совместное использование образовательных инициатив и технологических решений создает комплексный подход к обеспечению безопасности молодежи в цифровом пространстве.

2.9 Рекомендации для родителей и педагогов по предотвращению кибербуллинга

Родители играют важную роль в предотвращении кибербуллинга, особенно среди подростков. Согласно исследованию Pew Research Center, 59% подростков в США сталкивались с кибербуллингом, что подчеркивает необходимость активного участия родителей в мониторинге онлайн-активности своих детей. Родителям рекомендуется регулярно обсуждать с детьми их взаимодействие в интернете, обучать их основам безопасного поведения в сети и предупреждать о возможных рисках. Также важно использовать инструменты родительского контроля, которые позволяют ограничивать доступ к нежелательному контенту и отслеживать активность детей в интернете. Такие меры помогут родителям быть в курсе происходящего и вовремя реагировать на возможные угрозы.

Педагоги также играют ключевую роль в предотвращении кибербуллинга, особенно в школьной среде. Программа quot;Кибербезопасность в школахquot; в Великобритании показала, что обучение педагогов методам предотвращения кибербуллинга снижает количество инцидентов на 30%. Педагогам рекомендуется проводить образовательные мероприятия, направленные на повышение осведомленности учащихся о кибербуллинге и его последствиях, а также обучать их навыкам безопасного общения в интернете. Кроме того, важно создавать в школах атмосферу доверия, где ученики могут открыто рассказывать о своих проблемах и получать поддержку. Эти меры помогут минимизировать случаи кибербуллинга и создать более безопасную образовательную среду.

# Заключение

В ходе проведенного исследования были рассмотрены различные аспекты кибербуллинга и онлайн преступлений, включая их природу, причины и последствия. Было выявлено, что кибербуллинг представляет собой сложное явление, связанное с психологическими, социальными и культурными факторами. Анализ онлайн преступлений, таких как мошенничество, кража личных данных и распространение вредоносного контента, позволил определить их основные особенности и угрозы для пользователей.

Основные выводы исследования подчеркивают значимость комплексного подхода к решению проблем кибербуллинга и онлайн преступлений. Было установлено, что психологические и социальные аспекты играют ключевую роль в проявлении кибербуллинга, а технические меры и законодательные инициативы являются необходимыми для противодействия онлайн преступлениям. Также выявлена важность образовательных программ и осведомленности пользователей для повышения уровня безопасности в интернете.

На основе проведенного анализа рекомендуется усилить образовательные инициативы, направленные на повышение осведомленности пользователей о рисках и способах защиты в интернете. Развитие технологий для автоматического выявления и предотвращения кибербуллинга и онлайн преступлений также является приоритетом. Важно продолжать исследования в этой области, чтобы адаптировать существующие меры к изменяющимся условиям цифрового пространства и обеспечить безопасность пользователей.

# Список литературы

1. Акиньшина О.Н., Пирязева М.В., Анцева В.О. Проблема кибербуллинга: причины, способы противостояния, психологические последствия <https://phsreda.com/e-articles/10474/Action10474-106884.pdf>
2. Алиева А.М. Проблема кибербуллинга в образовательной среде // Студенческий электронный журнал «СтРИЖ». <http://strizh-vspu.ru/files/publics/1537963819.pdf>
3. Белковец О. С. Феномен кибербуллинга среди подростков в социальных сетях // Весці БДПУ. <https://elib.bspu.by/bitstream/doc/13866/1/216108.pdf>
4. Богомолова А. Г., Кот Е. А. Криминалистические аспекты кибербуллинга как формы деструктивного поведения в сети Интернет. <https://journals.kantiana.ru/upload/iblock/7fe/3_25-32.pdf>
5. Бочавер А.А., Хломов К.Д. Кибербуллинг: травля в пространстве современных технологий // Журнал Высшей школы экономики. — М., [https://psy-journal.hse.ru/data/2015/02/24/1090737958/Bochaver,%20Khlomov\_3\_2014\_177\_191.pdf](https://psy-journal.hse.ru/data/2015/02/24/1090737958/Bochaver%2C%20Khlomov_3_2014_177_191.pdf)
6. Дудников А.А. Предупреждение кибербуллинга в молодежной среде / <https://rep.vsu.by/bitstream/123456789/43812/1/224-226.pdf>
7. Егорова В.И. Гендерные исследования кибербуллинга // Психология. Историко-критические обзоры и современные исследования. <http://www.publishing-vak.ru/file/archive-psycology-2024-7/e1-egorova.pdf>
8. <https://magpk.ru/images/alias_vestnik_politeha/archive/vestnik_politekha_N_14.pdf#page=254>
9. <https://kalinovsky-k.narod.ru/b1/altay-2020.pdf#page=27>
10. <http://sno.mgppu.ru/sites/default/files/2020-06/%D0%A1%D0%B1%D0%BE%D1%80%D0%BD%D0%B8%D0%BA%20%D1%82%D0%B5%D0%B7%D0%B8%D1%81%D0%BE%D0%B2%20%D0%9A%D0%BE%D0%BD%D1%84.29.10.19%20%20%D0%B4%D0%BB%D1%8F%20%D0%A0%D0%98%D0%9D%D0%A6.pdf#page=131>
11. Каретина А.С., Назарова И.А., Денисова И.Е., Пушкина К.В. Буллинг и кибербуллинг как социальное явление /. <https://phsreda.com/ru/article/106927/discussion_platform>
12. Кирсанова Т. Я., Петрова С. С. Кибербуллинг в современном мире среди детей младшего возраста и подростков // Научно-практический электронный журнал Аллея Науки. <https://alley-science.ru/domains_data/files/5November2020/KIBERBULLING%20V%20SOVREMENNOM%20MIRE%20SREDI%20DETEY%20MLADShEGO%20VOZRASTA%20I%20PODROSTKOV.pdf>
13. Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы [Электронный ресурс] : материалы Всерос. науч.-практ. конф. / редкол.: С. А. Буткевич, И. А. Петрожицкая, А. В. Гончарова и др. ; под общ. ред. С. А. Буткевича. — Краснодар : Краснодарский университет МВД России, <https://www.prlib.ru/item/1978418>
14. Солдатова Г. У., Чигарькова С. В., Калинина К. Р. Психологические особенности участников ситуации кибербуллинга: анализ ролевого онлайн-поведения // Познание и переживание. <https://admin.inpsycho.ru/files/Science/PIP/2022-1/2022-1-03_Soldatova_soavt.pdf>
15. Халфина Р. Р. Агрессия подростков в интернете: троллинг и кибербуллинг // Доклады Башкирского университета. <http://dokbsu.ru/sites/default/files/pdf/2019/4/3/17_Khalfina_v1_349-354.pdf>
16. Хирина Е.В. Кибербуллинг в среде старшеклассников: особенности и последствия // Издательский дом «Среда». <https://elar.urfu.ru/bitstream/10995/121647/1/m_th_e.d.bachinina_2023.pdf>
17. Цифровое общество: проблемы и перспективы развития : сборник научных трудов по материалам Всероссийской научно-практической конференции <https://vgltu.ru/files/cifrovoe_obwestvo_problemy_i_perspektivy_razvitiya_2021.pdf>