Современные угрозы интернет-пространства: как помочь ребенку не потерять себя : информационно-аналитическая справка / Д.Е. Гуляев. — Москва, 2023. — 55 с.

Гуляев Дмитрий Евгеньевич,

Директор Центра по обеспечению прав молодежи в цифровом пространстве Университета имени О.Е. Кутафина (МГЮА)

Информационно-аналитическая справка
«Современные угрозы интернет-пространства: как помочь ребенку не потерять себя?»

1. ОБЩИЙ БЛОК

Безопасность и ее виды

В большинстве документов стратегического планирования и законов в сфере безопасности **понятие «безопасность»** определяется как состояние защищенности определенных объектов или интересов от угроз. Такой подход разделяется большинством российских исследователей проблем национальной и информационной безопасности.

В соответствии со Стратегией НБ 2021 **национальная безопасность** есть «состояние защищенности национальных интересов РФ от внешних и внутренних угроз» (пп. 1 п. 5).

В документах стратегического планирования и законодательстве Российской Федерации наблюдаются **различные подходы** к определению **видов безопасности**. В Стратегии НБ 2021 выделены государственная,

общественная, информационная, экологическая и иные виды безопасности (п. 26).

Выделение информационной безопасности (англ. information security) в системе видов безопасности является общепризнанным как в России, так и за рубежом.

Информационная безопасность и ее виды

Информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[1].

Согласно российскому законодательству **информационная безопасность детей** – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от

[1] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» https://www.garant.ru/products/ipo/prime/doc/71456224/?ysclid=lfjnta1n1s314429774

29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

В российской науке среди исследователей информационной безопасности долгое время доминировал **узкий подход** к ее пониманию как защиты информации и информационных систем.

В этой связи О.С. Макаров обоснованно сетовал на то, что «проблема информационной безопасности часто искусственно сужается до технических аспектов защиты информации, при этом опускаются, прежде всего, ее социально-гуманитарные аспекты»[2].

А.Д. Урсул определяет **информационную безопасность** как состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям.

Информационная безопасность – состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие[3].

Палитра современных угроз информационной безопасности чрезвычайно разнообразна. Она включает в себя как информационное измерение традиционных угроз безопасности (преступности, терроризма, военных действий), так и «чистые» информационные угрозы (сетевые атаки, применение вредоносного программного обеспечения, ложные новости).

Анализ всей совокупности имеющихся информационных угроз позволяет выделить **две основные группы таких угроз по критерию объектов воздействия:**

1) связанные с деструктивным информационно-психологическим воздействием на человека и общество;

---

[2] *Макаров О.С.* Актуальные аспекты обеспечения информационной безопасности государств – участников Содружества Независимых Государств: монография. Минск: Ин-т нац. безопасности Респ. Беларусь, 2013. С. 6.
[3] https://cyberleninka.ru/article/n/ponyatie-i-printsipy-informatsionnoy-bezopasnosti?ysclid=lfjd77muti644139636

2) связанные с вредоносным информационно-техническим воздействием на информационную инфраструктуру.

Таким образом, **выделяют информационно-психологическую безопасность и информационно-техническую (цифровую) безопасность.**

В действующем законодательстве РФ сформировались следующие **правовые институты** в структуре подотрасли правового обеспечения информационной безопасности:

1) защита информации, включая защиту отдельных видов информации ограниченного доступа;

2) защита критически важных объектов информационной инфраструктуры;

3) защита детей от информации, причиняющей вред их здоровью и развитию;

4) противодействие распространению противоправной информации в СМИ и сети Интернет.

Последние два пункта характеризуют сферу информационно-психологической безопасности[4].

Из книги «Цифровая гигиена» И. Ашманова и Н. Касперской:

Риски цифрового мира можно условно разделить на **два вида:**

1) **Электронные риски, или кибер-риски,** угрожающие самому устройству (смартфону, планшету, ноутбуку), установленным на нём программам, банковским счетам, паролям и т. п.

2) **Информационные** (они же контентные) риски, создающие угрозы сознанию владельца цифрового устройства: от развития цифровой зависимости, ухудшения когнитивных способностей до прямых атак на сознание.

[4] Диссертация Смирнова А.А. / Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации

- **К первой категории рисков** – кибер-рискам – относятся компьютерные вирусы, троянские программы, непрошеное рекламное программное обеспечение, тайно устанавливающееся на смартфон, шпионские программы, почтовый спам, разнообразные атаки на пользователя (разводки) с использованием социотехники, которые проводят вымогатели, шантажисты, финансовые мошенники. Все они могут привести к потере файлов, разрушению устройства, краже паролей, исчезновению денег с банковского счёта и т. п.

- **Вторая категория рисков** – информационные – включает возникновение цифровой зависимости от общения в социальных сетях, ухудшение когнитивных способностей, формирование клипового сознания, вовлечение в деструктивные группы, секты, экстремистские организации, а также пропаганду, «перепрошивку» сознания.

Обеспечение инф. Безопасности[5]

Правовое обеспечение информационной безопасности – это специальные законы, нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту личной информационной среды учащегося на законодательной и правовой основе, для реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию.

Нравственный и этический контроль подразумевает соблюдение школьниками при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики, которые складываются по мере распространения информационных технологий в современном информационном обществе.

[5] Богатырева Ю.И. / Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения // https://cyberleninka.ru/article/n/model-obespecheniya-informatsionnoy-bezopasnosti-shkolnikov-pri-sozdanii-infobezopasnoy-sredy-obrazovatelnogo-uchrezhdeniya?ysclid=lfl0carqiw974446169

Защита психики и здоровья ребенка – меры направлены на актуализацию потребности школьников в хорошем здоровье, физическом благополучии, как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и Интернет- зависимости среди учащихся. Педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности школьников.

Воспитательные меры по обеспечению ИБ – меры направленные на формирование культуры безопасности, ответственности за производимые действия в информационном пространстве, меры воспитания и укрепления духовно-нравственных ценностей, патриотизма, меры по подготовке родителей и педагогов к принятию позиции ребенка и помощи в его самореализации.

Техническое и программное обеспечение ИБ – это использование различных технических и программных средств, препятствующих нанесению материального или морального ущерба личной информации, программы родительского контроля, технические средств защиты информации.

Образование в области информационной безопасности – реализация образовательных программ в курсе школьных учебных предметов (ОБЖ и других), организация дополнительного образования учащихся во внеклассной работе по информационной безопасности, повышение квалификации педагогического состава, проведение тематических родительских собраний и встреч с интересными людьми.

Формирование информационной культуры школьников – через образовательную и воспитательную среду школы, которая определяется нами как компонент базовой культуры личности и характеристики человека, позволяющей ему эффективно выполнять все виды работы с информацией, понимать природу информационных процессов и осуществлять информационную рефлексию без ущерба для себя и окружающих.

2. ИНЫЕ ВИДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В то же время, в науке выделяются следующие виды информационной безопасности:

- Информационно-мировоззренческая безопасность
- Медиа-безопасность
- Когнитивная безопасность

Информационно-мировоззренческая безопасность

Является синонимом информационно-психологической безопасности.

Информационная безопасность личности является неотъемлемой частью информационной безопасности Российской Федерации и может рассматриваться **в двух аспектах:**

- как безопасность самой информации (персональных данных, личной и семейной тайны и т.д.)
- как защита от (деструктивной) информации

Информационно-мировоззренческая безопасность не сводима ни к одному из этих аспектов: она охватывает, прежде всего, второй аспект, т.к. предполагает защиту от информации, деструктивно влияющей на аксиосферу (мировоззрение) личности, его психологическое и психическое состояние , но также частично пересекается и с первым аспектом, т.к. распространение, например, сведений, составляющих личную или семейную тайну, может служить поводом для травли (буллинга) лица и даже доведения его до самоубийства.

Кроме того, можно выделить и **третий аспект** информационной безопасности, охватывающий свободу человека в информационном пространстве – право получать и распространять информацию, не нарушая права иных лиц.

Информационно-мировоззренческая безопасность предполагает защиту от манипулирования сознанием личности, насаждения симулякров и формирования, соответственно, псевдореальности, картины мира с искаженными или подмененными ценностями, установками и т.д., где во главу угла ставится культ агрессии к окружающим (собственно агрессивный дискурс) или к себе самому (депрессивно-аутодеструктивный дискурс).

Применительно к средствам массовой коммуникации **манипуляция** означает действия, направленные на программирование мнений, устремлений, целей и психических состояний масс с целью контроля над населением и его управляемостью.

Манипуляцию можно рассматривать как систему информационно-психологического воздействия, ориентированного на насаждение иллюзорного мировосприятия. Данная форма скрытого воздействия на сознание связана с отсутствием свободного волеизъявления индивида и способности принятия им собственных решений. **Конечная цель манипулятора** – сформировать специфическое отношение к объекту как к средству для достижения собственных целей; ввести адресата в заблуждение относительно характера подаваемой ему информации и т.д.

Таким образом, под **информационно-мировоззренческой безопасностью** нами предлагается понимать состояние защищенности личности, при котором отсутствует контентные и коммуникационные риски, связанные с причинением информацией вреда её здоровью и (или) физическому, психическому, духовному, нравственному развитию. Отметим, что в рамах данного исследования мы позволяем себе использовать понятия «информационно-мировоззренческая безопасности личности» и «информационно-мировоззренческая безопасность коммуникации» как синонимичные, основываясь на приеме метонимии: коммуникация выступает замещающим словом и обозначает процесс, в который вовлечена личность, чью безопасность необходимо обеспечить.

Медиа-безопасность

Термин нормативно не закреплен. Это западный термин, который является синонимом информационно-психологической безопасности (национальный термин).

В литературе представлены различные точки зрения понятия «медиа-безопасности».

В широком смысле медиа-безопасность – это деятельность, направленная на защиту интересов гражданского общества от появления и распространения недостоверной информации в сети Интернет, способной негативно повлиять на социальные процессы.

В узком смысле медиа-безопасность – это деятельность по обеспечению личной безопасности пользователя в сети Интернет, которая позволяет ему не только распознавать недостоверную информацию, но и, используя механизмы саморегуляции интернет-среды, предотвращать распространение вредоносной информации[6].

Искусственно возможно **разграничение терминов медиа-безопасность и информационно-психологическая безопасность.**

Понятие «медиабезопасность» выступает по отношению к понятию «информационно-мировоззренческая безопасность» более широким, т.к.:

- во-первых, охватывает в том числе информационные угрозы, не направленные на деструкцию мировоззрения человека, но нарушающие его права посредством распространения в медиа конфликтогенной и криминогенной информации (в т.ч. посягающей на его доброе имя, честь, достоинство, деловую репутацию ввиду дискредитирующеего, диффамационного, клеветнического характера информации);

[6] https://cyberleninka.ru/article/n/mediabezopasnost-kak-aktualnoe-napravlenie-mediaobrazovatelnoy-deyatelnosti?ysclid=lfjps17pow522630711

- во-вторых, медиабезопасность – состояние, которое необходимо обеспечить не только в отношении физических, но и в отношении юридических лиц.

Например, в инфополе высокотехнологичных проектов могут совершаться **следующие речевые действия**, образующие объективную сторону правонарушений (преступлений):

- диффамация (диффамационные речевые действия):

1) гражданско-правовая диффамация (ст. 152 ГК РФ);

2) уголовно-правовая диффамация: клевета (ст. 128.1 УК РФ), оскорбление представителя власти (ст. 319 УК РФ);

3) административно-правовая диффамация: оскорбление (ст. 5.61 КоАП РФ);

- фейкинг (фейкинговые речевые акты): злоупотребление свободой массовой информации (ст. 13.15 КоАП РФ)

- словесный экстремизм (экстремистские речевые действия): угроза совершения террористического акта (ст. 205 УК РФ), заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ).

Когнитивная безопасность

Этот вид безопасности входит в понятие информационно-психологической безопасности, как его составная часть.

Связано это с существованием **3-х уровней (установок) психологического восприятия**[7]**:**

- Поведенческого
- Когнитивного

[7] https://studme.org/383247/psihologiya/struktura_sotsialnoy_ustanovki_kognitivnyy_emotsionalnyy_povedencheskiy_komponenty?ysclid=lflj3m77gz833135517

- Аффективного (эмоционального)

Соответственно, **воздействие может оказываться на 3 уровня:**

1 – воздействие на поведение человека, направленное на достижение цели – конкретного поведения человека (совершения им конкретных действий)

2 – скрытое воздействие на разум человека, на «то, что он думает»: разрушение его системы ценностей и мировосприятия, создание ложной, искаженной картины восприятия мира, а впоследствии – «автоматический» выход личности на нужный (злоумышленнику) поведенческий уровень

3 – воздействие на эмоции человека

Соответственно, **когнитивная безопасность** – это деятельность, направленная на защиту личности от когнитивного воздействия (а именно на его разум, систему ценностей и мировосприятие).

Несколько иная точка зрения предполагает, что динамический подход предполагает выделение в структуре психики составляющих ее психических процессов, которые обычно подразделяются на **три основных вида:** когнитивные, эмоциональные и регулятивно-волевые. Статический подход исходит из выделения психических образований, являющихся результатами протекающих психических процессов[8].

[8] Диссертация Смирнова А.А. / Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации

Индивидуальные психические процессы и образования, составляющие структуру психики человека

Группа психических процессов	Психический процесс	Психические образования
Сознательные психические процессы и психические образования		
Регулятивно-волевые процессы	мотивация	потребности, мотивы, цели, интерес, желание, стремление, намерение
	воля	
	внимание[151]	–
Эмоциональный процесс	эмоциональный процесс	эмоции, чувства, настроение
Когнитивные процессы	ощущение	ощущения
	восприятие	перцептивные образы
	память	информация, воспоминания, представления памяти
	мышление	мысль, знание, понятие, суждение, умозаключение, решение
Бессознательные психические процессы и психические образования		
Регулятивно-волевые процессы	мотивация	несознаваемые побудители деятельности, неосознаваемые регуляторы способов выполнения деятельности (операциональные установки и стереотипы)
	воля	
	внимание	–
Эмоциональный процесс	эмоциональный процесс	аффекты
Когнитивные процессы	ощущение	проявления субсенсорного (подпорогового) восприятия, надсознательные явления
	восприятие	
	память	
	мышление	

3. ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ[9]

Информационно-психологическая безопасность (ИПБ) – составная часть системы информационной безопасности, представляющая собой состояние защищенности личности, социальных групп и общества от деструктивного информационно-психологического воздействия.

Принципиальные отличия ИПБ от традиционного блока информационной безопасности:

- Ее содержанием выступает **не защита информации, а защита от информации**. Защиту кого/чего? Прежде всего самого человека и общества в целом.

[9] Там же

- **Акцент на междисциплинарность** – связан с тем, что рассматриваемая предметная область ИПБ изначально носит гибридный характер и находится на стыке ряда сфер: информационных технологий, психологии и безопасности.

Приоритетным объектом правовой защиты от деструктивного информационно-психологического воздействия на уровне социальных групп выступают дети (несовершеннолетние) по причине их особой уязвимости, обусловленной их психологическими особенностями, включая некритичность восприятия информации, неустойчивость и эластичность ценностных ориентаций и поведенческих установок, высокой степенью бессознательного заражения эмоциональными состояниями, склонностью к подражанию поведению показанных героев, реализмом воображения.

Понятие **информационно-психологического воздействия (ИПВ)** охватывает весьма обширный круг явлений, связанных с оказанием психологического влияния на индивида и социум: от попыток воздействия в межличностном общении до широкомасштабных пропагандистских кампаний в политике, бизнесе или профилактической медицине.

Формы ИПВ:

- **Контент:** исследователи видят источник деструктивного воздействия на человека и социум в негативной (вредоносной) информации (письмо, телефон, СМИ, Интернет и др.).

- **Деструктивная коммуникация:** непосредственное или опосредованное техническими средствами общение между индивидами или группой лиц, оказывающее негативное влияние.

Грань между контентной и коммуникационной формами деструктивного ИПВ весьма тонкая, поскольку коммуникация между людьми также связана с передачей информации и последующим воздействием ее на человека.

Основным критерием их дифференциации является наличие прямого или опосредованного техническими средствами контакта между людьми – во второй группе такой контакт наличествует, в первой – отсутствует. Поэтому коммуникационные угрозы преимущественно связаны с межличностным или групповым общением, а контентные – с массовой коммуникацией.

Еще один аспект – **технические угрозы ИПБ,** связанные с негативным ИПВ на человека сигналов от технических устройств (направленное электромагнитное излучение, звуки определенной частоты и т.д.).

Таким образом, **деструктивное информационно-психологическое воздействие** включает в себя негативное влияние на личность и социальные группы деструктивного контента или коммуникации, а также сигналов от технических устройств, дистанционно воздействующих на психику человека через зрительные и слуховые сенсорные системы, создающее опасность причинения вреда интересам личности, общества и государства.

В то же время, «различные онлайн-риски сегодня имеют достаточно размытые границы, поэтому, выделяя отдельные главы по коммуникационным и контентным онлайн-рискам, мы к такому разделению подходим в некоторой степени условно, так как деятельность по вовлечению в террористические сообщества или так называемые «группы смерти» на данный момент относятся не просто к контентной или коммуникационной сфере – сегодня их уже можно обозначить **как контентно-коммуникационные риски»**[10]**.**

Контентные угрозы[11]

[10] Солдатова Г. У., Чигарькова С. В., Дренёва А. А., Илюхина С. Н. // Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. – М.: Когито-Центр, 2019. – 176 с.
[11] Диссертация Смирнова А.А. / Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации

Группа контентных угроз охватывает виды информации, имеющей негативный (вредный, опасный) характер.

Основные контентные угрозы ИПБ:

1) информация, пропагандирующая либо оправдывающая войну и иные международные преступления, терроризм;

2) информация, разжигающая ненависть и вражду в социуме;

3) информация, связанная с фальсификацией истории или осквернением исторической памяти;

4) информация, стимулирующая или содействующая совершению преступлений или иных общественно опасных действий;

5) ложная или искаженная информация;

6) информация, унижающая (порочащая) честь, достоинство или репутацию лица либо оскорбляющая общественную нравственность;

7) порнографический и иной сексуально откровенный контент;

8) информация устрашающего характера.

1) Пропаганда криминальных субкультур — распространение «информации о социокультурных ценностях у мира, направленной на формирование привлекательности криминального образа поведения (зачастую происходит в сообществах в социальных сетях).

Как выявить (признаки-маркеры)[12]:

- активное изучение и обсуждение материалов, содержащих идеологию субкультуры
- использование жаргона, жестов, символики, воспроизведение песен, текстов, касающихся субкультуры

[12] https://www.смкол.рф/docs/2020/Методические%20рекомендации%20по%20криминальным%20субкультурам%20(1).pdf?ysclid=lfl0fxomvy766041393

- манера использования «кличек»
- тематические музыкальные композиции («блатная музыка»)
- самостоятельное деление на группы, агрессивно противостоящие друг другу
- жестокое, насильственное отношение к представителям «чужой» группы
- четкая и понятная иерархия внутри таких групп, поддерживаемая насилием и жестоким обращением с представителями «низшей ступени»
- отсутствие чувства сострадания к людям, высмеивание слабых и беззащитных
- унижение и эксплуатация слабых, и представителей «низшей ступени» своей группы, глумление над ними

Способы противодействия *(правозащитный уровень):*

КоАП РФ:

- нарушение законодательства о свободе совести, свободе вероисповедания и о религиозных объединениях (ст. 5.26);
- незаконные действия по отношению к государственным символам Российской Федерации (ст. 17.10);
- мелкое хулиганство (ст. 20.1);
- нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования (ст. 20.2);
- пропаганда либо публичное демонстрирование нацисткой атрибутики либо символики, либо атрибутики или символики экстремистских организаций либо иных атрибутики либо символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами (ст. 20.3);
- производство и распространение экстремистских материалов (ст. 20.29)

УК РФ:

- ст. 136 УК РФ — нарушение равенства прав и свобод человека и гражданина;
- ст. 148 УК РФ — воспрепятствование осуществлению прав на свободу совести и вероисповеданий;
- ст. 149 УК РФ — воспрепятствование проведению собрания, митинга, демонстрации, шествия, пикетирования или участию в них;
- ч. 4 ст. 150 УК РФ — вовлечение несовершеннолетнего в совершение преступления;
- ст. 212 УК РФ – массовые беспорядки;
- ч. 1 п. б ст. 213 УК РФ — хулиганство и др.

АУЕ («Арестантско-уркаганское единство», «Арестантское уголовные единство», «Арестантский уклад един»)[13] – деструктивная молодежная субкультура, основной идеей которой является пропаганда криминального образа жизни, совершение преступлений и финансирование преступной деятельности. а также навязывание криминальных законов, т. н. «понятий», в противовес государственным законам.

Для онлайн-сообществ АУЕ-тематики характерны:

- «мода на оружие»;
- романтизация и оправдание криминального и асоциального образа жизни (употребление алкоголя, наркотиков, половая распущенность);
- пропаганда насилия над сотрудниками правоохранительных органов;
- фото и видеозаписи сцен насилия;
- романтизация биографий лидеров преступного мира, т.н. воров в законе.

[13] В.Д. Никишин, А.Я. Осипов, Е.А. Борисов, И.Ю. Сундиев «Выявление и профилактика деструктивной пропаганды в молодежной и подростковой среде»

АУЕ-пропаганда может сопровождаться следующими тезисами:

- противопоставление субкультуры АУЕ конституционному строю, государственному строю, действующей власти, с возведением в статус гаранта Конституции (согласно негласным правилам преступного мира – это воровские понятия) лица, занимающего высшее положение в преступной иерархии – вора в законе, а также низложение полномочий сотрудников правоохранительных органов

- оправдание, обоснование радикальных криминальных действий по отношению к представителям государственной власти, а также призывы к совершению данных действий

- возбуждение ненависти и вражды по отношению к правоохранительным органам РФ и их представителям, а также призывы к совершению актов насилия по отношению к ним

- демонстрация нацисткой атрибутики и символики, запрещенной на территории РФ, в целях противопоставления идеологии АУЕ действующему государственному строю

- пропаганда моды на оружие как средство совершения преступлений и атрибут «повседневной» жизни

- постулирование элитарности последователей субкультуры АУЕ: изображения с короной, а также образами, ассоциирующимися с царями и иными верховными представителями власти

- создание иллюзии «законности» осуществляемой последователями АУЕ деятельности не с точки зрения уголовного кодекса и иных нормативых правовых актов, а с точки зрения православных и моральных норм путем:

1) изображения классических атрибутов криминальной жизни: алкоголя, оружия, азартных игр, иных неотъемлемых элементов разгульной и криминальной жизни – вместе с антагонистскими символами: православными крестами, иконами и т.п., что является реализацией

психологического приема по введению в заблуждение относительно честности представителей AVE («Мы соблюдаем все заповеди, кроме одной - «Не укради», иконы и кресты – оберег на удачу во время совершения жестоких преступлений, покровительство «свыше»)

2) «перемежение» деструктивного контента с контентом, пропагандирующим семейные, патриотические и иные традиционные ценности

Со стороны администраторов ресурсов АУЕ размещается контент патриотической направленности, содержащий нормы морали традиционного российского общества, однако это делается с целью создания лояльности незнакомой с тематикой АУЕ аудитории к этой субкультуре, что вводит пользователей в заблуждение и провоцирует прирост новых подписчиков. В постах действует манипулятивная пропаганда идей криминальных сообществ посредством размещения контента, признанного общей моралью, на тему семьи, патриотизма, здорового образа жизни и человеческого равенства «вперемешку» с криминальными идеями. Для неокрепшего подростка такая манипуляция является опасной, так как подросток может решить, раз следует пропаганда общепринятых норм, то и криминальные идеи тоже являются общепринятыми, либо не являются деструктивными. **То есть мы наблюдаем психологическую манипуляцию детским и подростковым сознанием через соответствующие ассоциации.**

К признакам вовлеченности лица в субкультуру АУЕ относятся:

- использование в разговоре фраз «Фарту, масти, АУЕ*», «АУЕ, жизнь ворам» «АУЕ, шпана», «АУЕ, братва» и т.п.;
- использование «кличек» в обращениях;
- ношение атрибутов криминальной субкультуры (оружие, четки, карты и т.д.); размещение изображений (постеров и т. п.) криминальной направленности, соответствующих символов;
- прослушивание аудиозаписей АУЕ-тематики;

- участие в сборе средств в т.н. «общак»;
- участие в совершении преступлений, уважаемых в уголовной среде: кражи, грабежи, разбои, вымогательства;
- использование различных жестов (в т.ч. при фотографировании) для определения «посвященности» или принадлежности к криминальному движению АУЕ
- использование аббревиатур и лозунгов «ШПАНА А.У.Е.», «С.С.Ж.В.»
- использование символа АУЕ – восьмиугольной «розы ветров» («воровская звезда»)

Важным маркером вовлеченности лица в субкультуру АУЕ является жизнь «по понятиям», которая базируется на **следующих принципах:**

1. Преданность и поддержка воровской идеи
2. Недопустимость никаких контактов с правоохранительными органами
3. Быть честными по отношению друг к другу
4. Вовлечение в свою среду новых членов
5. Отказ от сотрудничества с любыми властными структурами
6. Никогда не давать показания
7. Никогда не признавать вину
8. Не работать ни при каких условиях
9. Пополнение общака для помощи осуждённым, находящимся в местах лишения свободы
10. Чтить родителей (особенно мать)
11. Учить правильной жизни младших ребят, разъяснять, что такое правильные понятия
12. Непримиримое отношение к доносительству

Вербовка в экстремистские и террористические сообщества[14]

Для методики вовлечения молодежи в экстремистскую деятельность со стороны ИННО характерными являются такие признаки, как:

- «тотальный» мониторинг социально-политической ситуации на всей территории России для определения наиболее нестабильных (с экономической и политической точек зрения) регионов, в которых молодежь выступает в качестве основной движущей силы протестной активности
- ориентированность преимущественно на студенческие коллективы гуманитарного профиля, активисты которых готовы участвовать в различных структурах, оппозиционных политическому и экономическому курсу руководства Российской Федерации
- постоянная и значительная финансовая поддержка вовлекаемых лиц
- стимулирование желания молодежи участвовать в политической борьбе преимущественно в форме протестной деятельности;
- неприкрытая спекуляция лозунгами об отстаивании социальной справедливости;
- использование на завершающей стадии вовлечения перспективной молодежи приглашений за рубеж, особенно в те страны Европы, где иностранным организациям удалось задействовать молодежный студенческий потенциал для «свержения» неугодных Западу «антидемократических» режимов
- пропаганда необходимости «цивилизовать Россию» путем внедрения любыми средствами «западных ценностей»;
- настойчивые рекомендации давать броские названия объединениям, которые способны привлечь внимание молодежи (например, «Пора», «Хватит!», «Смена» и др.)

[14] В.Д. Никишин, А.Я. Осипов, Е.А. Борисов, И.Ю. Сундиев «Выявление и профилактика деструктивной пропаганды в молодежной и подростковой среде»

- соблюдение сетевого принципа при создании оппозиционных молодежных движений, широчайшее использование новых информационных тех-пологий и социальных сетей и др.

На подготовительном этапе вербовщики МТО (терроризм) осуществляют:

а) поиск (в том числе в социальных сетях, блогосфере) отдельных молодых людей, подходящих им по своим личным и деловым качествам;

б) подбор и изучение групп молодежи, сформированных по какому-либо признаку (например, этнонациональному), чаще с радикальными установками;

в) сбор и изучение характеризующей информации на лицо, группу (а чаще на лидера группы);

г) привлечение внимания лица (группы) с помощью рекламы, пропаганды;

д) первичное знакомство.

Расчет вербовщиков прост – сначала увлечь, затем удовлетворить возрастную потребность в самоутверждении (для девушек – найти спутника жизни), сознательное желание молодого человека быть принятым в круг себе подобных и понятных по духу, настроениям и переживаниям.

За предварительным этапом следует **основной**, в ходе которого применяется запланированный комплекс **специфических методов по вовлечению** лица или группы лиц в террористическую организацию, которые применяют при этом сильное групповое давление и манипулирование потребностями человека, в результате чего начинаются изменения базисных ценностей личности. Главная цель данного этапа заключается в окончательном включении объекта в структуру террористического формирования.

Наиболее часто используется **убеждение** – метод воздействия на сознание личности через обращение к ее собственному критическому суждению.

Моральное давление на основе компрометирующих человека перед окружением сведений довершает процесс вовлечения в террористическую деятельность.

Суть методов вовлечения, не связанных с насилием, состоит в постепенном, на первый взгляд ненавязчивом внедрении какой-либо простой идеи в сознание молодого человека. В психологии такие методы имеют название **«манипулятивные приемы».** Они дают множество возможностей влиять на сознание человека, особенно в условиях, когда он пользуется ограниченной и искаженной информацией. Поэтому для внедрения в сознание объекта нужной информации субъекту манипулирования (вербовщику) важно всегда поддерживать состояние, при котором вербуемый испытывает дефицит информации. При этом для достижения большего эффекта наряду с другими приемами почти всегда применяется дезинформирование вовлекаемого (вербуемого).

КЕЙС[15]: МКУ

- В связанных с МКУ Telegram-каналах Краснов объясняет, что к насилию его подтолкнули детские травмы. Но не раскаивается, а, наоборот, говорит, что нападения кажутся ему «веселыми».

- Себя они называют «маньяками и убийцами», а свои акции – «жертвоприношениями».

- Думаете, я могу поведать для вас все, что знаю? – гласит Истинному Времени знакомая тамбовчанина Андрея С. – В базе идеологии у них была ксенофобия, другими словами «утиль».

[15] https://rus-republic.com/2021/03/30/m-k-y-kylt-ybiistv-kotoryi-byl-sozdan-skinhedami-v-dnepre-i-ego-posledovateli-v-rossiiskoi-federacii

— Что означает «утиль»?

— Утилизация переселенцев.

- Данный момент и такие ему он называет «приступами садизма», позже обрисовывает «свист ветра и шепот деревьев». И рассказывает, что «заплакал от счастья», когда осознал, что сделал.

2) Аутоагрессивное (направленное на самого себя) поведение, обусловленное явным или скрытым намерением умереть и проявляющееся в виде фантазий, мыслей, представлений или действий, направленных на самоповреждение или самоуничтожение *(культура суицидального поведения, группы смерти и т.п.)*.

Группы смерти – это молодежная деструктивная субкультура, изначально созданная и распространяемая в социальных сетях в Интернете, основной целью которой является доведение участников групп через игру до нанесения себе самоповреждений и в конце концов – до самоубийства.

Для «групп смерти» характерны:

- публикации изображений внутренних органов, крови
- видеозаписи насилия и убийств
- изображения оккультных символов
- иногда встречаются нейтральные изображения полуобнаженных девушек и / или милых аниме-персонажей
- видеозаписи и фотографии самоубийств

Как выявить (признаки-маркеры)[16]:

- безнадёжность – отсутствие надежды на улучшение состояния и возможность помощи со стороны окружающих

[16] https://www.gokpb.by/text/sucide_scale_for_social.pdf?ysclid=lfl0khhwul534705242, http://socobslugivanie.by/index.php?option=com_content&view=article&id=106&Itemid=106

- признаки «прощания»: раздача долгов, подарков, написание завещания, «прощальных» писем
- суицидальные попытки ранее: чем больше количество и выше тяжесть парасуицидов, тем выше вероятность дальнейшего суицидального поведения
- плохое настроение, снижение интереса к обычным для данного человека занятиям, контактам и развлечениям, снижение работоспособности, повышение утомляемости и т.д.
- наличие стрессовой ситуации
- отсутствие поддержки (проживание в одиночестве, замкнутый образ жизни или наличие враждебного, осуждающего окружения)
- подписка на соответствующие сообщества (в социальных сетях)

Также к признакам вовлеченности лица в «группы смерти» относятся[17]:

- наличие эмоциональных нарушений: потеря аппетита или импульсивное переедание;
- бессонница или повышенная сонливость;
- частые жалобы на соматические недомогания (боли в животе, головные боли, постоянную усталость, сонливость);
- нехарактерное пренебрежение к своему внешнему виду;
- чувство одиночества, бесполезности, вины или грусти;
- ощущение скуки при проведении времени в привычном окружении или выполнении работы, которая раньше приносила удовольствие;
- уход от контактов, изоляция от друзей и семьи, превращение в человека «одиночку»;
- нарушение внимания со снижением качества выполняемой работы;

[17] В.Д. Никишин, А.Я. Осипов, Е.А. Борисов, И.Ю. Сундиев «Выявление и профилактика деструктивной пропаганды в молодежной и подростковой среде»

- погруженность в размышления о смерти, отсутствие планов на будущее;
- внезапные приступы гнева, зачастую возникающие из-за мелочей

Вовлечение в «группы смерти»:

1. Возбуждение любопытства к тематике через потребление депрессивного медиаконтента условных трех уровней (воронка вовлечения): 1) слабо-депрессивный (фон-завлечение); 2) депрессивный; 3) прямая пропаганда суицида

2. Появление новых «друзей» у подростка: приставление 2-3 кураторов, 1) которые по легенде обычно проживают в других регионах в другом часовом поясе (поэтому подросток вынужден общаться с ними в ночное время, нарушая режим); 2) один из которых нередко позиционируется представителем противоположного пола (и в дальнейшем инициирует секстинг («обмен» интимными фото- и видеоматериалам) с целью последующего шантажа.

3. Выявление проблем подростка (через переписку), получение личной информации о нем и семье, оказание подростку моральной поддержки («бомбардировка любовью»: только мы тебя понимаем).

4. Приглашение в «круг избранных», в закрытое сообщество, в игру.

5. Введение в игру (простые задания: проснуться в 4.20 и смотреть шок-контент, проснуться в 4.20 и пойти на крышу, целый день смотреть шок-контент). Продолжение игры (усложняющиеся задания), например: Проснуться в 4.20. Порезать вдоль вен руку (неглубоко). Только три пореза. Порезать губу.Протыкать руку иголкой. Залезть на мост. Залезть на кран. Сидеть вниз ногами на краю крыши. В 4.20 утра пойти на рельсы. Ни с кем не общаться (методика «КАРУСЕЛЬ»). Возможны и задания от кураторов: убить животное; убить человека; прислать интимные фотографии и т.п.

6. Кризис в игре (манипуляция психологическими проблемами, усиление акцентов): куратор приказывает преодолеть в себе страхи, на финише смертельной игры подростку называют дату смерти и внушают, что он должен смириться.

7. Завершение игры (активация «триггера») – совершение суицида.

Индикаторы вовлечения в «группы смерти» можно определить как на основе онлайн-исследования страницы исследуемого, так и на основе офлайн-проявлений.

При анализе страницы пользователя изучается название и описание его профиля (возможна отсылка к поиску групп смерти, желания участвовать в игре), подписки на сообщества, музыкальные композиции, размещенные на его странице, видеозаписи, а также непосредственно размещаемые им публикации (депрессивный и суицидальный контент). Необходимо детально изучить группы и паблики, на которые он подписан.

Способы противодействия *(правозащитный уровень):*

- ст. 110.1 УК РФ – Склонение к совершению самоубийства или содействие совершению самоубийства
- ст. 110 УК РФ – Доведение до самоубийства

КЕЙС: Выдержки из интервью, которое «Филипп Лис» дал под диктофонную запись порталу Санкт-Петербург.Ру за несколько дней до ареста, и которое было опубликовано на сайте в день его задержания (15.11.2016):

Так, давай с самого начала. Когда все началось, как все было организованно и как ты дошел до того, что стал толкать людей на суицид?

Сначала? Есть люди, а есть биомусор. Это те, кто не представляет никакой ценности для общества и несет или принесет обществу только вред.

Я чистил наше общество от таких людей. Началось в 2013 году. Тогда я создал «F57» (одно из названий «групп смерти» «ВКонтакте») Просто создал, посмотреть, что будет.

Ты использовал смерть Рины Паленковой (16-летняя девушка под никнеймом Рина Паленкова совершила самоубийство 23 ноября 2015 года и стала одним из символов суицидального движения)?

Это моя первая суицидница. У меня даже где-то есть ее сигна (фотография с персональной подписью — прим. ред.). Скину тебе как-нибудь, если найду

Чем провинилась Рина? Она сделала что-то очень плохое?

Возможно.

Что было после смерти Рины?

Работали все мои группы: «F57», «F75», «F58» и так далее. Привлекали людей, они проходили этапы. Как это все работает: есть группа с депрессивным контентом, которая погружает человека в нужную атмосферу. В этих группах есть ссылки на другие. Проходя по этим ссылкам, человек натыкается на закрытое сообщество, где все и разворачивается. Начинается игра. Нужно выполнять задания, рассказывать о себе, общаться. В ходе этого общения становится понятно, кто есть кто. Дальше я иду с человеком в скайп, погружаю его в транс и узнаю какие-то вещи из его жизни, после чего принимаю решение. В какой-то момент нужно подтолкнуть подростка к тому, чтобы он не спал ночью. Здоровый режим для ребенка: лечь спать в 21:00, встать в 8:00. Если режим нарушить, то и психика становится более доступной к воздействию.

Ты будешь продолжать?

Да. Сейчас готовы уйти 28 человек. Это мой относительно новый проект «D28». Ажиотаж вокруг истории мне очень мешает, я жду, когда все утихнет, и спокойно продолжу. Не могу пока рассказать, это секрет.

Как психолог оцени свои собственные действия. Ты никогда не думал о том, что у тебя «не все дома»?

У меня биполярное расстройство личности, а то, чем я занимаюсь, связанно с моим тяжелым детством. Меня и мать избивал старший брат. Часто били на улице. Уверен, что все это оказало большое влияние.

3) Распространение фейковой (ложной) информации.

Насыщение информационного пространства недостоверными фактами создает почву для формирования определенного отношения к определенным людям, явлениям, процессам и к действительности в целом. Таким образом можно не только добиться от людей желаемого поведения, но и поменять их взгляд на мир, создать вместо достоверной картины мира его карикатурный образ.

Как выявить (признаки-маркеры) – как понять, что это фейк:

- Отсутствие указания на источник информации, ссылка на некие анонимные (осведомленные) круги.
- Кричащие, кликбейтные, провокационные, категоричные заголовки.
- Нагнетание автором страха, возмущения, гнева или других эмоций.
- Сенсационная или якобы рассекреченная информация.
- Орфографические ошибки
- Вырванные из контекста высказывания известных личностей.
- Односторонняя подача информации.

Способы противодействия *(правозащитный уровень):*

- ст. 13.15 КоАП РФ «Злоупотребление свободой массовой информации»;
- ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма»;

- ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан»;
- ст. 207.2 УК РФ «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия»;
- ст. 207.3, согласно которой запрещено публичное распространение под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооруженных Сил РФ в целях защиты интересов РФ и ее граждан, поддержания международного мира и безопасности, а равно содержащей данные об исполнении государственными органами РФ своих полномочий за пределами территории РФ в указанных целях; ст. 354.1 УК РФ «Реабилитация нацизма» (запрещено отрицание фактов, установленных приговором Международного военного трибунала).

Правила проверки достоверности информации в Интернете[18]:

1. Относись критично к любой информации в Интернете.

2. Красиво сделанный дизайн сайта – еще не повод верить всему, что на нем написано.

3. Если ты что-то узнал в Сети, найди источник информации, узнай, кто ее автор.

4. Задумайся, какова позиция автора сайта, на котором ты нашел информацию. Спроси себя: что тебе хотят доказать и во что заставить поверить?

5. Задумайся, единственная ли это возможная точка зрения. Какие мнения или идеи отсутствуют на сайте?

6. Следуй правилу трех источников: прежде чем поверить в какой-либо факт, проверь еще как минимум два других источника информации.

[18] Солдатова Г. У., Чигарькова С. В., Дренёва А. А., Илюхина С. Н. // Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. – М.: Когито-Центр, 2019. – 176 с.

7. Будь осторожен, используя факты, которые ты еще не проверил.

НЕКОТОРЫЕ ФОРМЫ ДЕСТРУКТИВНОГО ПОВЕДЕНИЯ (УГРОЗ)

Деструктивные риски и угрозы можно разделить следующим образом:

- содержательные (выступает как непосредственные угрозы с присущей только им характеристикой)
- формальные (выступают как формы донесения деструктивной информации)

Так, к формальным можно отнести хеппислепинг и треш-стримы.

1) Хеппислепинг (счастливое хлопанье, радостное избиение) — название происходит от случаев в английском метро, где подростки избивали прохожих, тогда как другие записывали это на камеру мобильного телефона.

Сейчас это название закрепилось за любыми видеороликами с записями реальных сцен насилия. Однако в большинстве случаев это видео с избиением сверстников, которые сопровождается уничижительными комментариями со стороны обидчиков. Эти ролики могут просматривать тысячи людей без согласия жертвы.

Способы противодействия *(правозащитный уровень):*

- ст. 20.3.1 КоАП РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства);
- ст. 282 УК РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства).

Составы за реальные действия: ст. 111 УК РФ (умышленное причинение тяжкого вреда здоровью); ст. 112 УК РФ (умышленное

причинение средней тяжести вреда здоровью); ст. 115 УК РФ (умышленное причинение легкого вреда здоровью); ст. 116 УК РФ (побои).

2) Треш-стримы являются крайне опасным способом (формой) распространения деструктивной пропаганды среди молодежи. В них показываются такие опасные для жизни человека модели поведения как «зацепинг» («трейнхоппинг») – способ передвижения, проезд на автосцепных устройствах, на крыше или на межвагонных буферах пассажирских поездов, а также на других, не приспособленных для провоза пассажиров частях транспортных составов (электрички, поезда метро, автобуса); «стритрейсинг» - опасные незаконные автогонки на общественных дорогах и другое.

Ответственности в законодательстве РФ не указано, предлагается для этого изменить ст. 282 УК РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства). Существует законопроект по противодействию треш-стримам, а также экспертиза Совфеда предлагает признать треш-стримы отягчающим обстоятельством при назначении наказания.

Коммуникативные угрозы[19]

Группа коммуникационных угроз охватывает негативное ИПВ в ходе контакта между людьми. В отличие от предыдущей группы, для которой основным источником угроз являются массмедиа, коммуникационные угрозы исходят из межличностной и групповой коммуникации. Она может включать в себя непосредственные формы «живого общения» (разговор, участие в концерте, демонстрации) либо опосредованные применением

[19] Диссертация Смирнова А.А. / Формирование системы правового обеспечения информационно-психологической безопасности в Российской Федерации

технических средств (разговор по телефону, переписка в интернет-чате, общение в режиме видеозвонка или видеоконференции и т.п.).

Негативные проявления устной коммуникации (оскорбление, запугивание, принуждение и др.) издревле рассматривались в качестве угроз. Вместе с тем особую опасность формы негативной коммуникации приобрели именно в настоящее время в условиях широкого проникновения мобильной связи, социальных сетей и мессенджеров. Новые технические средства коммуникации **сделали возможными свободное общение между малознакомыми людьми,** которые к тому же имеют возможность скрывать или искажать свою личность.

Описанные тенденции повлекли бурный рост коммуникационных угроз ИПБ в последние два десятилетия. Среди них **наиболее актуальными можно назвать:** вербовку в террористические и экстремистские организации, вовлечение в совершение преступлений, подстрекательство аутодеструктивного поведения, обман в целях завладения имуществом (мошенничество), коммуникацию, разжигающую ненависть или вражду; негативную сексуальную коммуникацию. Отдельно стоит упомянуть такие **формы речевой агрессии**, как троллинг, флейминг и буллинг, получившие очень широкое распространение в онлайн-среде, особенно социальных сетях.

1) Кибербуллинг – связан с обширным списком негативных явлений, таких как харассмент и хейтинг, эксклюзия (остракизм), стигматизация (приписывание негативных и осуждаемых качеств, «клеймение»), дегуманизация (отказ признавать за лицом человеческого достоинства, перевод его в разряд вещей), киберсталкинг, угрозы и т.д. То есть это обобщающее понятие для многих угроз.

Кибербуллинг — вид буллинга, у них крайне много общего, однако есть и принципиальные различия. *Они описаны в книге Андрея Афанасьева «Дети интернета. Что они смотрят, и кто ими управляет»:*

1. Иллюзия безнаказанности и анонимности. Кибербуллинг осуществляется в цифровой среде с помощью цифровых инструментов, что создает дополнительную иллюзию анонимности и вседозволенности для участников, затрудняет раскрытие фактов травли, но совсем не исключает этого.

2. Длительность воздействия. После окончания уроков и в выходные дни жертва буллинга может абстрагироваться от травли, прийти в себя, при кибербуллинге травля в выходные и праздники не прекращается. Кибертравля может продолжаться годами, находить отклики уже во взрослой жизни.

3. Охват. При буллинге издеваться может пара-тройка человек, класс, группа людей, в случае кибербуллинга это может быть совершенно другое куда более обширное количество людей, которых даже сосчитать будет проблематично.

4. Переход в другой класс или даже школу не решит проблему. Перейдя в другую школу, ребёнок-жертва кибербуллинга может столкнуться с тем, что там про него уже все всё знают.

5. Сложность определения признаков травли. Когда над ребёнком издеваются в школе, то это всегда видно – синяки, слезы, нервное состояние. В случае кибербуллинга всё сложнее. Ребёнок может находиться уже на грани, но про это может никто не знать.

6. Жертвой может стать кто угодно. В Интернете травят любых детей, даже тех, кого в офлайне травить мало бы кто решился. Но здесь все не так просто, об этом мы поговорим чуть позже.

7. Специфические формы проявления.

Признаки жертвы:

- ребенок негативно относится к учебному заведению или иному месту, которое он систематически должен посещать, использует любую возможность, чтобы туда не ходить;
- если он все же идет – то выбирает более длинные маршруты, опаздывает на уроки;
- у него нет или практически нет друзей, он не ходит в гости и к нему не заходят сверстники;
- возвращается подавленный;
- плачет без очевидной причины;
- ничего не рассказывает о коллективе;
- становится грубым, раздражительным и вспыльчивым по отношению к окружающим и особенно к младшим по возрасту и родителям;
- плохо спит и ест;
- могут присутствовать синяки и ссадины на лице или теле, может часто «рваться» одежда, могут постоянно «рваться» или «пачкаться» тетради, учебники и т.д.

Способы противодействия *(правозащитный уровень):*

- ст. 128.1 УК РФ (клевета) – распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающего его репутацию. Отдельным составом выделяется клевета в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, сотрудника органов принудительного исполнения РФ (ст. 298.1 УК РФ);
- ст. 5.61 КоАП РФ (оскорбление),
- ст. 20.1 КоАП РФ (мелкое хулиганство),
- ст. 20.3.1 КоАП РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства);
- ст. 282 УК РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства).

Рекомендации[20]:

Следует обратить внимание обучающихся на следующие моменты:

- в интернет-травле они могут оказаться как по одну, так и по другую сторону;
- любая переписка может храниться очень долго (минимум полгода), к тому же любые материалы сейчас можно сохранить, создав архив;
- даже при использовании VPN-сервисов, предотвращающих отслеживание активности в Интернете, есть другие способы установления зачинщика интернет-травли

Как противостоять киберагрессии и кибербуллингу? Общие рекомендации для подростков и молодежи[21]:

- Помните, что информация, попавшая в Интернет, может стать доступной множеству людей и быть использована против вас.
- Добавляя незнакомых френдов в социальной сети, подумайте, насколько это безопасно. Они могут стать как ресурсом для развития, так и возможным источником агрессивных действий.
- Используйте настройки приватности, чтобы защитить информацию о себе от ненужных глаз. Не забывайте про техническую безопасность: используйте надежные пароли, регулярно меняйте их и никому не сообщайте.
- Если по отношению к вам проявляют агрессию, не реагируйте. Ваша эмоциональная реакция – это то, чего добивается агрессор.
- Сохраняйте доказательства. Делайте скриншоты или распечатки сообщений, сохраняйте доказательства действий обидчика. Эти

[20] Интернет-безопасность детей: методические рекомендации // https://nro.center/wp-content/uploads/2019/10/rekomendacii.pdf?ysclid=lfl0x5n0gs786939284

[21] Солдатова Г. У., Чигарькова С. В., Дренёва А. А., Илюхина С. Н. // Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете: Учебно-методическое пособие. – М.: Когито-Центр, 2019. – 176 с.

доказательства помогут защитить себя при обращении к классному руководителю, администрации школы или полиции.

- Отправляйте обидчиков в «черный список», блокируйте.
- Сообщайте об агрессорах модератору или службе поддержки сайта или социальной сети, используя, например, кнопку «Пожаловаться».
- Не оставайтесь с агрессией наедине – расскажите об этом тому, кому доверяете. Обратитесь за помощью: к родителям или знакомому взрослому, в службу психологической помощи.
- Не будьте равнодушными. Если вы видите, что кого-то обижают, то поддержите его. Оцените опасность ситуации, если вы понимаете, что не можете самостоятельно помочь или для вас это может быть небезопасно, обратитесь к специалисту, которому доверяете.
- Размещая пост, репост, статусилифото,подумайте, немогутли они обидеть других людей. Представьте, что бы вы чувствовали, оказавшись на месте того, кого вы хотели обидеть или обидели.

2) Кибергруминг можно охарактеризовать как налаживание виртуального взаимодействия с ребенком с целью получения его интимных снимков, видеозаписей или же иных видов сексуально направленных действий.

Как выявить (признаки-маркеры)[22]:

Что это кибергруминг:

- Злоумышленник много пишет. Это происходит очень часто и разными способами — в Facebook, Instagram, Whatsapp и других мессенджерах.

[22] https://sch37.edu-penza.ru/files/Метод%20рекомендации%20по%20профлактике%20виктимного%20поведения.pdf

- Злоумышленник просит держать общение в секрете. Просит никому не рассказывать о разговорах, чтобы это было их «особенным секретом», говорит о доверии.
- Злоумышленник пытается разузнать побольше. Расспрашивает, может ли взять компьютер или телефон ребенка кто-то еще, в какой комнате он находится во время общения. В общем, обо всем, что даст понять, могут ли их разоблачить взрослые.
- Злоумышленник начинает отправлять свои сексуальные изображения. Это всегда начинается очень незаметно. Например, может бросить фото и спросить: «Тебя когда-нибудь так целовали?» или «Новый фотосет. Не слишком?»
- Злоумышленник пытается шантажировать. Очень настойчиво просит отправить свои откровенные снимки или видео в ответ. Если получает отказ, сильно расстраивается, обижается, грозится навредить себе.
- В случае, когда ребенок поддается на провокацию, злоумышленник может пригрозить, что разместит их в интернете, покажет всей школе, родителям и т. д., если тот не пришлет новые более откровенные фото и видео или деньги.

Что обучающийся подвергается кибергрумингу:

- Резко становится замкнутым, грустным, напряженным, и это состояние продолжительное;
- Начинает по-другому вести себя с учителями, сверстниками, родителями;
- Теряет интерес к учебе, соответственно его успехи стремительно снижаются;
- Рассредоточен, часто сидит за компьютером или в телефоне, после чего еще более расстроен;
- Быстрее тратит карманные деньги, под любыми предлогами пытается получить их увеличение.

Способы противодействия *(правозащитный уровень):*

- ст. 135 УК РФ (развратные действия).

Рекомендации:

- В первую очередь **нужно быть осторожным с Интернет-знакомствами**. Нередко самый дружелюбный собеседник оказывается скрытым агрессором. В таких случаях главное вовремя распознать сущность своего «друга». Так, если вначале общения он раскрывается вам, посвящает вас в свои замыслы, делится впечатлениями и планами, и все это в короткий срок, то это должно наталкивать на сомнения в его искренности, так как в «здоровых» отношениях, как правило, заложен определенный период для перехода на этап доверия и полного взаимопонимания.

- Следующим шагом обычно является **спешная «заморозка» отношений**, когда начинаются негативные прецеденты. Это может быть исключение из зоны внимания т.е., когда человек начинает резко обрывать контакты и без объяснения причин пропадает. Другой формой могут выступать начальные проявления агрессии – недвусмысленные намеки на недостатки, шутливые насмешки и т.д. Таким образом, осуществляется плавный переход к иным и более интенсивным формам унижения.

- Жертва, которую застали врасплох, наиболее остро ощущает негативные эмоции и переживания от автора агрессии, который раньше вел себя дружелюбно. Именно поэтому **важно поддерживать стабильную самооценку**. Это основополагающее правило, которое способно нейтрализовать действия любого агрессора.

- Иные правила являются универсальными и сводятся к простому **соблюдению сетевого этикета.** Достаточно быть вежливыми, не поддаваться на провокации и соблюдать базовые правила Интернет-безопасности.

КЕЙС[23]: Рассказывает Константин Игнатьев, «Лаборатория Касперского»:

«Пятнадцатилетняя старшеклассница из Барнаула познакомилась в соцсети с мужчиной 30 с лишним лет. У них завязался диалог. Потом они встретились в реальности, он за ней ухаживал и, в конце концов, уговорил вступить с ним в половую связь. Более того, снял этот процесс на видео, сделал множество фотоснимков девочки в обнаженном виде, а затем начал ее шантажировать. Две недели она скрывала произошедшее от родителей, но потом все-таки призналась. Родители обратились в полицию, преступника нашли и осудили. Правда, срок он получил условный — 5 лет. Через какое-то время семья девочки переехала в Москву — они это давно планировали, а происшествие только ускорило переезд.

Но на этом история не закончилась. Мужчина снова попытался выйти с девочкой на связь и для этого создал в соцсети «ВКонтакте» ее фейковый аккаунт с фотографиями. Староста класса, в котором училась девочка, нашел этот якобы ее аккаунт и добавил его в группу класса. В результате злоумышленник узнал, где она учится, и снова начал ей угрожать. Но, к счастью, у него ничего не получилось.

Благодаря тому, что героиня этой истории тесно и доверительно общалась с родителями, которые ее всячески поддерживали, она прошла это испытание, хотя и не без травм, но все же сохранив здравый рассудок».

3) Кибersталкинг является одной из наиболее опасных форм кибербуллинга, он представляет собой преследование лица посредством Интернета, в т.ч. в социальных сетях. Кибersталкинг возможен только лишь при наличии односторонней коммуникации.

[23] С. Макаров, Прекрасный, опасный, кибербезопасный мир // https://shkolaizluchinskaya-r86.gosweb.gosuslugi.ru/netcat_files/30/69/Makarov_Opasnyy_prekrasnyy_kiberbezopasnyy_mir.pdf

Преследователь на протяжении долгого времени донимает жертву различными оскорблениями и угрозами, следит за ее Интернет-следами, стремится донести свою негативную оценку на опубликованный ею материал или же на те факты из ее жизни, о которых становится ему известно.

Преследователь буквально вовлечен в жизнь своей жертвы. Такая форма несёт персонифицированный характер.

Как выявить (признаки-маркеры):

Что обучающийся подвергается кибersталкингу:

- Они получают телефонные звонки, сообщения или электронные письма в необычное время.
- Они получают подарки от людей, которых вы не знаете.
- Они явно расстроены, напуганы или плачут после выхода в Интернет.

Способы противодействия *(правозащитный уровень):*

- ст. 5.61 КоАП РФ (оскорбление)
- ст. 137 УК РФ (нарушение неприкосновенности частной жизни)
- ст. 272 УК РФ (неправомерный доступ к компьютерной информации)

4. ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Эта конструкция **законодательно в РФ не закреплена**, а выработана искусственным путем.

Кибербезопасность, также известная как цифровая безопасность, — это практика защиты цифровых сведений, устройств и ресурсов. Это включает личные данные, учетные записи, файлы, фотографии и даже деньги.

Цифровая безопасность – состояние защищённости цифровой информации, цифровой инфраструктуры и цифровых технологий, обеспечивающее защиту конституционных прав и свобод человека и гражданина, законных интересов субъектов цифровых правоотношений от реальных и потенциальных угроз[24].

К угрозам цифровой безопасности относятся[25]:

- компьютерные вирусы,
- троянские программы,
- непрошеное рекламное программное обеспечение, тайно устанавливающееся на смартфон,
- шпионские программы, почтовый спам,
- разнообразные атаки на пользователя (разводки) с использованием социотехники, которые проводят вымогатели, шантажисты, финансовые мошенники.

Все они могут привести к потере файлов, разрушению устройства, краже паролей, исчезновению денег с банковского счёта и т. п.

Угрозы

1) Вирусный контент[26].

Меняет или полностью блокирует доступ к персональному компьютеру. В такой ситуации пользователю часто приходит требование осуществить перевод или отправить СМС на предлагаемый номер для восстановления пароля. В других случаях компьютер может подвергнуться заражению «трояном», который делает доступными для злоумышленников личные данные.

[24] https://cyberleninka.ru/article/n/cemanticheskiy-analiz-termina-tsifrovaya-bezopasnost?ysclid=lfjs3rapuv329865772
[25] И. Ашманов, Н. Касперская, Цифровая гигиена
[26] Интернет-безопасность детей: методические рекомендации // https://nro.center/wp-content/uploads/2019/10/rekomendacii.pdf?ysclid=lfl0x5n0gs786939284

ПРИМЕР: В сети «ВКонтакте» это обычно выглядит так: пользователю предлагают пройти по ссылке на сайт, который на самом деле является мошенническим, и там узнать все интересующие его тайны. На этом сайте предлагается скачать ПО для взлома учетных записей в социальной сети «ВКонтакте». Однако после клика на кнопку загрузки под видом «программы-взломщика» начинается скачивание троянца-вымогателя. После этого на рабочем столе компьютера появляется окно с предложением отправить СМС-сообщение на короткий номер, чтобы получить программу для доступа к личным данным пользователей сети «ВКонтакте». Одновременно троянец блокирует работу системы до тех пор, пока вымогатели не получат выкуп в виде СМС.

«Лаборатория Касперского» рекомендует при обнаружении СМС-блокера на компьютере не идти на поводу у мошенников и не отправлять сообщения, а удалить назойливый баннер с рабочего стола с помощью бесплатного сервиса на сайте «Лаборатории Касперского». Данная услуга доступна также и через мобильное устройство.

Рекомендации:

- Обсудите с ребятами, что нельзя переходить по опасным ссылкам, принимать какие-либо сомнительные соглашения.
- Для защиты компьютера нужно устанавливать специальные защитные программы и фильтры.
- Для надежной защиты лучше использовать лицензионное программное обеспечение с актуальными обновлениями. Устанавливать необходимо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия антивируса.
- Стоит относиться с осторожностью к скачиванию программных продуктов из файлообменных сетей и торрентов.
- Подозрительные файлы не открывайте и не сохраняйте.
- Не отвечайте на сомнительные рассылки.

- И главное — не посещайте ресурсы с неоднозначной репутацией, которые вызывают у вас (антивирусной программы) любые подозрения.

2) Фишинг (получение доступа к логинам, паролям, банковским данным)[27].

Мошенники организуют рассылку сообщений якобы от имени банка со ссылками на поддельные страницы официальных сайтов. Вводя свои персональные данные (номера банковских карт, логины, пароли), жертва неосознанно передает конфиденциальную информацию мошенникам. А те, в свою очередь, используют сведения для завладения денежными средствами.

Рекомендации:

Для предупреждения школьников о подобных схемах мошенничества можно:

- рассказать о специализированных интернет-ресурсах проверки сайтов на факты совершения мошеннических действий (например, сайт https://довериевсети.рф/) и других сервисах контроля репутации сайта на предмет мошеннических действий (негативные отзывы, жалобы на сайт, проверка на вирусы). Напомнить, что достоверный сайт обязательно содержит сведения об авторах и их контактные данные;

- обратить внимание детей на то, что нельзя вводить данные банковских карт на сомнительных сайтах интернет-магазинов (cvc/cvv-код, срок действия, номер карты);

- напомнить, что никому не стоит передавать или выкладывать в Сеть конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес прописки и фактического места жительства, слишком личные фотографии.

[27] Там же

3) Утечка (кража) данных — это нарушение безопасности, при котором чувствительные, защищенные или конфиденциальные данные копируются, передаются, просматриваются, крадутся, изменяются или используются лицом, не имеющим на это права.

4) Взлом аккаунта (в социальных сетях и т.п.) — вид интернет-мошенничества, цель которого - обманом заставить человека предоставить конфиденциальную информацию (например, пароли доступа к аккаунтам в социальных сетях) для дальнейшего вымогательства денег или рассылки спама от лица взломанного пользователя.

АВТОРСКИЙ КЕЙС

ФАБУЛА

- Пятиклассник Виктор получил по электронной почте приглашение от друга Паши вступить в его команду и принять участие в интернет-игре, доступ к которой откроется по ссылке в письме.
- Виктор перешел по ссылке.
- Экран заполонила форма подтверждения участия, куда нужно было обязательно внести личную информацию, а также логин и пароль от одной из социальных сетей, чтобы в дальнейшем упростить вход в игру.
- Виктор заполнил форму, ведь в письме Паша его о ней уже предупредил.
- Через мгновение Виктор оказался в игре, правда, Пашу он в ней так и не нашел.
- Спустя сутки на самом интересном месте у персонажа игры закончилась бесплатная экипировка, и Виктор получил новое письмо с предложением ее купить и новой ссылкой.
- Пятиклассник перешел по ней, но указывать данные банковской карты родителей все же не стал.

- Еще через несколько дней Виктору на почту стали поступать новые письма: уже не со ссылками, а с требованиями оплатить проведенное в игре время и даже угрозами в адрес него самого и его семьи.
- Виктор их проигнорировал, и в скором времени одну из его страниц в соцсетях взломали, легко изменили пароль и разослали всем друзьям от его имени сообщения с просьбой перевести по указанному номеру карты деньги на «лечение больной бабушки».
- В окружении Виктора оказалось много неравнодушных людей, которые, к сожалению, так и не вернули свои деньги.
- Доступ к аккаунту Виктор тоже так и не смог восстановить.

ОШИБКИ

- Приступив к игре, он так и не нашел там своего друга, что должно было натолкнуть на мысль о том, что стоит связаться с Пашей и уточнить, присылал ли он такое письмо (правило: Осторожно относитесь к поступающей почте, не открывайте письма с сомнительных адресов, не переходите по ссылкам от незнакомых отправителей. В письме могут содержаться вредоносные программы, ссылки на них и т.д.)
- Перейдя по ссылке, Виктор внес в «регистрационную» форму логин и пароль от социальной сети и личную информацию (правило: необходимо бережно и внимательно относиться к своим паролям и личным данным).
- Если злоумышленники легко зашли в аккаунт Виктора и поменяли пароль, у пятиклассника отсутствовала функция двухфакторной аутентификации, т.е. определения пользователя сервиса (в частности, социальной сети) с помощью разных типов запроса данных.
- Получив письмо с предложением купить экипировку для персонажа, Виктор без сомнения перешел по ссылке.

ПОЛОЖИТЕЛЬНЫЕ ЯВЛЕНИЯ

- Он не стал вводить данные банковской карты родителей
- Проигнорировал угрозы, которые стали ему поступать

РЕКОМЕНДАЦИИ К СИТУАЦИИ

- При поступлении сомнительных предложений стоит все же убедиться, что с Вами переписывается именно этот человек: позвонить или написать ему «по другим каналам».
- Вводить свои логины и пароли в незнакомые формы нельзя
- Создавая пароли, нужно помнить, что они должны быть достаточно длинными и надежными. Не стоит использовать для этого даты рождения. На различных платформах нужно использовать разные пароли, и лучше запоминать их, а не записывать.
- При поступлении угроз не следует отвечать, вступать в полемику или иной диалог со злоумышленниками. Ведь их первоочередная цель – спровоцировать.
- Было бы лучше сохранить все переписки (а лучше – сделать скриншоты) и как можно скорее обратиться к родителям, которые могли бы обратиться с ними в правоохранительные органы.

ОБЩИЕ РЕКОМЕНДАЦИИ

Необходимо проводить с учениками тематические беседы,

рассказывать о существующих угрозах безопасности их данных и устройств и способах противодействия.

5. СОВЕТЫ И РЕКОМЕНДАЦИИ ДЛЯ ПЕДАГОГОВ[28]

Анализ литературы дает основание утверждать, что **процесс обучения информационной безопасности целесообразно начинать со школы.** Поэтому важно проанализировать информационную безопасность школьника, **как педагогическую проблему**, цель решения которой есть педагогически направляемый процесс развития у ребенка знаний об информационной угрозе и умения противостоять ей для уменьшений последствий психического и нравственного воздействия.

Самым эффективным механизмом информационной безопасности несовершеннолетних может стать работа по формированию осознанного самостоятельного умения учащихся выбирать безопасную информацию. Лучший фильтр, который может обеспечить безопасность ребенка в сети и решить многие другие проблемы – в голове самого ребенка, а взрослому нужно только настроить этот фильтр.

1) ПРЕВЕНТИВНЫЕ МЕРЫ[29]:

1. Беседы с обучающимися и их родителями (превентивного характера), проведение тематических мастер-классов:

Задачи по формированию у современного школьника навыков и умений позитивного и полезного взаимодействия с информационной средой **решается как на уроке, так и во внеурочной деятельности.**

Для целенаправленной работы по формированию осознанного самостоятельного умения учащихся выбирать безопасную информацию, **в образовательном учреждении необходимо организовывать** часы общения, беседы, практикумы, тренинги и другие мероприятия по снижению у

[28] Склямина, М. Ю. Обеспечение информационной безопасности учащихся в системе общего образования // Молодой ученый. — 2015. — № 6.4 (86.4). — С. 52-55. — URL: https://moluch.ru/archive/86/16381
[29] Там же

обучающихся уровня тревожности, формированию адекватной самооценки, навыков безопасного поведения в ситуациях, угрожающих их жизни и здоровью в Интернете.

В школах необходимо проводить классные часы или психологические беседы со всеми учащимися на темы «Суицид», «Доведение до самоубийства». Подросткам необходимо разъяснять существование таких групп, их направленность и конечно, последствия совершения самоубийства, особенно лицам, подпадающим под группу риска (более склонным к совершению суицида)[30].

Так, в отношении фейков, педагог может дать ребенку следующие советы:

- Критически относиться к любой информации
- Не публиковать записи, в которых не уверены и др.

В рамках занятий по интернет-безопасности можно[31]:

- рассказать о том, почему не стоит выкладывать подробную информацию о себе, номер телефона и электронной почты;
- напомнить, что не нужно часто «чекиниться», то есть проставлять привязки к месту действия, выкладывая фотографии;
- можно провести инструктаж по поводу общения с незнакомыми людьми в Сети, научить говорить четкое «нет» на предложения списаться по электронной почте, созвониться, а тем более встретиться;
- провести разъяснительную работу о том, что нельзя раскрывать информацию о себе незнакомым людям, доверять сведения личного характера человеку, которого никогда не видел вживую и т.д.

[30] Коновалова, Ю. А. Доведение до самоубийства несовершеннолетних с использованием информационно-телекоммуникационных технологий // Молодой ученый. — 2022. — № 45 (440). — С. 138-140. — URL: https://moluch.ru/archive/440/96229

[31] Интернет-безопасность детей: методические рекомендации // https://nro.center/wp-content/uploads/2019/10/rekomendacii.pdf?ysclid=lfl0x5n0gs786939284

2. Разработка и реализация программ развития, воспитательных компонентов в образовательных организациях

3. Активное вовлечение несовершеннолетних в культурную, спортивную и общественную жизнь (внеурочная деятельность)

Умело спроектированное воспитательное пространство школы, организация занятости детей и подростков социально–значимой деятельностью является действенным способом обеспечения информационной безопасности.

Повышению информационной компетентности подрастающего поколения способствует участие школьников в областных конкурсах, конкурсе творческих работ по информатике и информационным технологиям, привлечение детей и подростков к изданию школьных газет, работе телестудий, разработке сайтов. Проводимые мероприятия дадут больший результат, если педагог будет привлекать родителей учащихся и повышать их компетенцию в вопросах информационной безопасности детей и подростков, через родительские собрания или ежемесячные родительские встречи.

4. Обеспечение доступности дополнительных программ и создание условий в образовательных организациях для работы творческих объединений по интересам для несовершеннолетних и молодежи, в том числе для лиц с трудностями в социальной адаптации

5. Осуществление мер по реализации программ и методик, направленных на формирование законопослушного поведения несовершеннолетних и молодежи

6. Оказание психолого-педагогической, медицинской и социальной помощи подросткам и молодежи, испытывающим трудности в освоении основных общеобразовательных программ, в их развитии и социальной адаптации

2) ПРЕСЕКАТЕЛЬНЫЕ МЕРЫ:

1. Беседы с обучающимися (пресекательного характера)
2. Предупреждение о возможном привлечении к юридической ответственности
3. Сообщение родителям обучающегося с целью определения дальнейших действий с несовершеннолетним (определения дальнейшей траектории педагога и родителя)
4. Консультации со школьным психологом (пресекательного характера; для оказания помощи ребенку-жертве)

Так, в случае наличия суицидального поведения:

- обеспечить немедленное наблюдение (при наличии признаков)
- наладить контакт с родственниками и другими эмоционально значимыми лицами: родственники и/или другие близкие люди должны быть поставлены в известность о суицидальных намерениях или действиях индивида
- обеспечить контроль над доступностью средств суицида (открытые окна, острые предметы, медикаменты и др.)
- проконсультировать о предоставляемой помощи: индивидуальные психологические консультации, психологические консультации анонимно по «телефону отзывчивости»

5. Разъяснение мер реагирования (мер самозашиты, обращения в правоохранительные органы и т.п.)

ОБЩИЕ РЕКОМЕНДАЦИИ[32]

Педагогам для обеспечения интернет-безопасности **учащихся 10-15 лет необходимо:**

[32] https://shkolaartezianskaya-r08.gosweb.gosuslugi.ru/roditelyam-i-uchenikam/poleznaya-informatsiya/informatsionnaya-bezopasnost/

- познакомить учащихся с ответственным, достойным поведением в Интернете;
- рассказать об основных опасностях и правилах безопасного использования сети Интернет;
- убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;
- объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;
- убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им.
- ознакомь с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу **с учащимися старших классов** по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации. Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

- Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.
- Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование модерируемых

(контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.

- Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь.
- Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.
- Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- Обсудите с подростками азартные сетевые игры и связанный с ними риск.

ПРИМЕР №1: На сегодняшний день **в школах Санкт-Петербурга реализуются различные методики организации** информационно безопасного образовательного процесса, основанные на включении вопросов информационной безопасности в уроки по ОБЖ. Одними из первых таких проектов стали «Поднимайся по лестнице компьютерной безопасности», который был проведен в гимназии № 272, «Информационная зависимость и ее профилактика», реализуемый в школе № 625, и ряд других.

ПРИМЕР №2: … школа стала одной из первых в Москве, где **ввели регламент пользования гаджетами:** их не запрещают, но и не разрешают пользоваться бесконтрольно. В регламенте мы обговариваем, в каких учебных ситуациях ребенок может пользоваться гаджетами (например, можно искать информацию для презентации на уроке), а в каких это делать нельзя (например, пока передвигаешься по школе или ешь в столовой). Также у нас, как и во всех московских школах, установлены контент-фильтры, которые блокируют информационные угрозы для школьников.

Если ребенок пользуется школьным вай-фаем, он не попадет на сайты, противоречащие российскому законодательству, и не увидит контент 18+. Фильтры действуют на всех — на учительские компьютеры тоже. При этом важно не запугивать детей: мы хотим донести, что интернет — не страшное, а полезное пространство, которое при соблюдении правил безопасности может принести немало хорошего[33].

ИНТЕРЕСНЫЕ МАТЕРИАЛЫ ДЛЯ ПЕДАГОГОВ

Интернет-ресурсы для педагогических работников:

- http://www.fid.su/projects/deti-v-internete сайт Фонда Развития Интернет.
- http://content-filtering.ru/ сайт «Ваш личный интернет», советы, рекомендации для детей и родителей по безопасной работе в Интернет.
- http://www.ligainternet.ru/ Лиги безопасного Интернета.
- http://ppt4web.ru/informatika/bezopasnyjj-internet.html презентации о безопасном Интернете.
- http://www.microsoft.com/ru-ru/security/default.aspx сайт Центра безопасности Майкрософт.
- http://www.saferunet.org/children/ Центр безопасности Интернета в России.
- https://edu.tatar.ru/upload/images/files/909_029%20Orangepdf Безопасно и просто: родительский контроль. — Буклет
- Урок в 9–10 классах. Профилактика интернет-зависимости «Будущее начинается сегодня» http://festival.1september.ru/articles/612789/ Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы.
- Материалы (буклет, презентация и текст) для бесед профилактике игровой и интернет-зависимости у детей и подростков на сайте

[33] https://snob-ru.turbopages.org/snob.ru/s/entry/193482/

Министерства образования и науки Республики Татарстан: http://mon.tatarstan.ru/prof_internet_zavisimosti.htm

- http://www.nachalka.com/node/950 Видео «Развлечение и безопасность в Интернете»
- http://i-deti.org/ портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы
- http://сетевичок.рф/ сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности
- http://www.igra-internet.ru/ — онлайн интернет-игра «Изучи Интернет – управляй им»
- http://www.safe-internet.ru/ — сайт Ростелеком «Безопасноть детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам