ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 17. ТЕМА 1.17 ОПАСНОСТИ, СВЯЗАННЫЕ С КОММУНИКАЦИЕЙ В ЦИФРОВОЙ СРЕДЕ

1. Поведенческие риски в цифровой среде и их причины

Поведенческие риски в цифровой среде представляют собой совокупность угроз, возникающих в процессе межличностной коммуникации пользователей посредством информационно-телекоммуникационных сетей и способных нанести вред физическому, психическому, социальному и репутационному благополучию личности. В отличие от технических рисков (вредоносное ПО, взлом, фишинг), поведенческие риски обусловлены не технологическими уязвимостями, а действиями самих пользователей — как жертвы, так и агрессора.

Концепция формирования и развития культуры информационной безопасности граждан Российской Федерации, утверждённая распоряжением Правительства РФ от 22.12.2022 № 4088-р, относит к психологическим угрозам информационной безопасности травлю в цифровом пространстве, пропаганду насилия, национализма, распространение недостоверной информации и иной вредоносный контент. Документ особо подчёркивает уязвимость граждан в возрасте до 18 лет, которая обусловлена возрастными особенностями, отсутствием необходимых знаний в области информационной безопасности и регулярным свободным использованием сети «Интернет», приводящим к ложному ощущению безопасности.

К числу основных причин поведенческих рисков относятся:

• **Анонимность коммуникации.** Возможность создания фейковых аккаунтов и использования вымышленных персональных данных снижает у агрессора ощущение неотвратимости наказания, а у жертвы — способность адекватно оценить намерения собеседника.

• **Эмоциональная уязвимость пользователей.** Лица, находящиеся в состоянии стресса, одиночества, депрессии или испытывающие потребность в признании, формируют группу повышенного риска для манипулятивного воздействия. infourok.ru +1

• **Недостаток критического мышления.** Ограниченный жизненный опыт, незрелость оценочных способностей и неустойчивость эмоциональной сферы, характерные для подросткового возраста, снижают способность распознать манипуляцию и противостоять ей.

• **Иллюзия безопасности цифровой среды.** Привычный, повседневный характер использования цифровых устройств формирует у пользователя ложное чувство контроля над ситуацией и снижает бдительность.

• **Отсутствие верификации собеседника.** В отличие от офлайн-коммуникации, цифровая среда не требует подтверждения реальной личности собеседника, что открывает возможности для имперсонации — выдачи себя за другое лицо.

2. Опасные персоны: имитация близких социальных отношений

Одной из наиболее опасных форм коммуникационных угроз в цифровой среде является имитация близких социальных отношений — целенаправленное установление доверительного контакта между злоумышленником и жертвой под видом дружбы, наставничества, романтической привязанности или профессионального покровительства. Данный феномен охватывает несколько типов деструктивного взаимодействия.

Груминг (кибергруминг) — систематический процесс установления доверительных отношений взрослого с несовершеннолетним через цифровые каналы коммуникации с целью последующей эксплуатации. Грумер может выдавать себя за сверстника, разделять интересы жертвы, проявлять эмоциональную поддержку. Процесс включает следующие этапы: выбор жертвы (как правило, уязвимой — имеющей сложные

отношения в семье, испытывающей одиночество), установление дружеского контакта, развитие отношений, оценку риска разоблачения, формирование ощущения исключительности отношений и, наконец, включение сексуального или иного эксплуатационного содержания.

В российском Уголовном кодексе отсутствует специальная статья, криминализующая груминг как самостоятельное деяние. Однако действия, совершаемые на различных этапах груминга, подпадают под ряд статей УК РФ: статья 135 «Развратные действия» (включая переписку сексуального характера с несовершеннолетним, демонстрацию изображений половых органов), статья 132 «Насильственные действия сексуального характера», статья 242.1 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», статья 150 «Вовлечение несовершеннолетнего в совершение антиобщественных действий», статья 137 «Нарушение неприкосновенности частной жизни».

Социальная инженерия в широком смысле — использование психологических манипуляций для получения доступа к конфиденциальной информации, деньгам или для вовлечения жертвы в противоправную деятельность. Вербовщики и мошенники создают иллюзию заботы, хвалят жертву, проявляют интерес к её проблемам, обещают быстрое решение проблем. Классический приём — изоляция жертвы от близких: «не рассказывай родителям, они тебя не поймут и запретят общаться».

Имперсонация — выдача себя за знакомого, родственника или должностное лицо. Злоумышленник может использовать данные, полученные из открытых источников (профили в социальных сетях), чтобы детально воспроизвести обстоятельства жизни жертвы и её знакомых, после чего запросить личную информацию, пароли или финансовые средства.

3. Неосмотрительное поведение и коммуникация в Сети как угроза для будущей жизни и карьеры

Репутационно-правовые риски представляют собой потенциальные негативные последствия, возникающие в результате онлайн-активности пользователя в прошлом или настоящем. Публикации ненадлежащего контента могут привести к отчислению из образовательной организации, увольнению с работы, шантажу со стороны третьих лиц или возбуждению уголовного дела, если онлайн-активность будет расценена как противоправная.

Цифровой след, формируемый каждым действием пользователя в сети, сохраняется практически бессрочно. Информация, размещённая в социальных сетях, мессенджерах, на форумах, может быть скопирована, сохранена и использована спустя годы — при поступлении в образовательную организацию, при трудоустройстве, при прохождении проверки для допуска к государственной службе, при рассмотрении кандидатуры на руководящую должность.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает, что информация, распространяемая без соблюдения установленных ограничений, может быть признана запрещённой к распространению на территории Российской Федерации, а страница, содержащая такую информацию, — внесена в Единый реестр доменных имён и сайтов, содержащих информацию, распространение которой запрещено.

Федеральный закон от 08.08.2024 № 216-ФЗ внёс изменения в закон № 149-ФЗ, установив, что доступ к информации может ограничиваться не только федеральными законами, но и актами Президента РФ. На владельца социальной сети возложена обязанность выявления информации, оскорбляющей человеческое достоинство и общественную нравственность, выражающей явное неуважение к обществу, содержащей изображение действий с признаками противоправных, в том числе насильственных, и распространяемой из хулиганских, корыстных или иных низменных побуждений.

К числу наиболее распространённых форм неосмотрительного поведения, создающих долгосрочные риски, относятся:

• публикация интимных фотографий и переписки, которые впоследствии могут быть использованы для шантажа;

• размещение оскорбительных комментариев, клеветы, угроз — деяний, подпадающих под статьи 5.61, 5.61.1 КоАП РФ и статьи 128.1, 119, 137 УК РФ;

• публикация материалов, оправдывающих противоправное поведение, — основание для ограничения распространения в соответствии со статьёй 5 Закона № 436-ФЗ;

• распространение экстремистских материалов — основание для привлечения к ответственности по Федеральному закону от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;

• участие в публичных конфликтах, троллинге, флейминге — формах коммуникации, способных нанести репутационный ущерб и повлечь правовые последствия.

4. Травля в Сети: методы защиты

Кибербуллинг (сетевая травля) — систематическая, повторяющаяся агрессия, направленная на конкретного человека с использованием электронных форм контакта и включающая оскорбления, запугивание, социальное бойкотирование, распространение личной информации без согласия владельца, публикацию интимных фотографий и видео.

В российском законодательстве отсутствует специальная норма, предусматривающая санкции за кибербуллинг как самостоятельное правонарушение. Однако действия, составляющие объективную сторону сетевой травли, квалифицируются по нескольким статьям КоАП РФ и УК РФ.

Административная ответственность:

• **Статья 5.61 КоАП РФ** — оскорбление, в том числе совершённое публично с использованием сети «Интернет». Штраф для физических лиц — от 3000 до 5000 рублей.

• **Статья 5.61.1 КоАП РФ** — клевета, распространение заведомо ложных сведений, порочащих честь и достоинство.

• **Статья 20.1 КоАП РФ** — мелкое хулиганство, включая распространение в сети «Интернет» информации, выражающей в неприличной форме оскорбление человеческого достоинства и общественной нравственности.

Уголовная ответственность:

• **Статья 128.1 УК РФ** — клевета.

• **Статья 137 УК РФ** — нарушение неприкосновенности частной жизни.

• **Статья 119 УК РФ** — угроза убийством или причинением тяжкого вреда здоровью (при условии, что потерпевший реально опасается высказанных угроз).

• **Статьи 110–110.1 УК РФ** — доведение до самоубийства, склонение к самоубийству.

• **Статья 138 УК РФ** — нарушение тайны переписки и иных сообщений (при взломе электронной почты и аккаунтов с последующим распространением материалов личного характера).

• **Статья 272 УК РФ** — неправомерный доступ к компьютерной информации.

Кроме того, статья 15.1 Закона № 149-ФЗ предоставляет прокурору право обращаться в суд с иском о признании информации запрещённой и включении страницы в Единый реестр доменных имён, содержащих запрещённую информацию.

Методы защиты от кибербуллинга:

1. **Настройка параметров конфиденциальности.** Ограничение доступа к странице в социальных сетях: просмотр постов и фотографий — только для друзей,

закрытие возможности комментирования для незнакомых лиц, запрет на отметку на фотографиях.

2. **Фиксация доказательств.** Сохранение скриншотов оскорбительных сообщений и комментариев, аудио- и видеозаписей. Письменные оскорбления в сети «Интернет» подлежат нотариальному заверению для использования в качестве доказательства в суде.

3. **Блокировка и жалоба.** Использование функций блокировки агрессора в социальных сетях и мессенджерах, подача жалобы администрации платформы с указанием причины (оскорбляющий контент, экстремизм, порнография, призывы к насилию).

4. **Обращение в Роскомнадзор.** При публикации персональных данных жертвы в открытом доступе — подача обращения через сайт или приложение Роскомнадзора. Размещение персональных данных без согласия субъекта является нарушением Закона и подлежит устранению держателем сайта.

5. **Обращение в правоохранительные органы.** При угрозах, вымогательстве, шантаже — подача заявления в полицию. При отказе в возбуждении дела — обжалование в прокуратуре или суде.

6. **Эмоциональное невовлечение.** Отказ от вступления в перепалку с агрессором. Эмоциональная реакция жертвы является основной целью агрессора; её отсутствие лишает его мотивации.

7. **Гражданско-правовая защита.** Лицо, в отношении которого распространены сведения, порочащие честь, достоинство и деловую репутацию, вправе требовать в суде опровержения и компенсации морального вреда.

5. Деструктивные сообщества и деструктивный контент: признаки

Деструктивные сообщества в цифровой среде — это организованные объединения людей, в основе существования которых лежит идеология, противоречащая ценностям общества и государства, деформирующая нравственный облик личности и проявляющаяся в противоправном поведении.

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (в действующей редакции) устанавливает исчерпывающий перечень видов информации, запрещённой для распространения среди детей. К ней относится, в частности, информация, побуждающая к совершению действий, представляющих угрозу жизни и здоровью, в том числе к самоубийству; обосновывающая или оправдывающая допустимость насилия; содержащая изображение сексуального насилия; оскорбляющая человеческое достоинство и общественную нравственность; пропагандирующая педофилию; оправдывающая противоправное поведение.

Классификация деструктивных сообществ в социальных сетях:

1. **Группы, пропагандирующие экстремистскую и террористическую идеологию** — террористические группировки, движения, признанные террористическими на основании решений Верховного суда РФ.

2. **Группы, пропагандирующие опасные увлечения** — зацепинг, опасные квесты, трэш-стримы, шок-контент.

3. **Группы, пропагандирующие причинение вреда себе или окружающим** — селфхарм, пиплхейт, депрессивно-суицидальные группы.

4. **Группы, пропагандирующие криминальную субкультуру** — например, «Арестантское уголовное единство» (АУЕ), признанное экстремистской организацией решением Верховного суда РФ от 17.08.2020. Участие в деятельности данного движения подпадает под статью 282.2 УК РФ.

Ключевые признаки деструктивного сообщества:

• **Маскировка под безобидные интересы.** Группы, имеющие вид спортивных, игровых, музыкальных сообществ, могут являться каналами вербовки в экстремистские или криминальные структуры.

• **Культивирование ощущения исключительности.** Подростку внушается, что только он и его «новые друзья» понимают «истину», а остальное общество — «стадо» или «враги».

• **Требование секретности.** «Не рассказывай родителям о наших беседах, они тебя не поймут» — классический приём изоляции жертвы от поддержки.

• **Постепенное изменение лексикона.** Появление специфических, часто выдуманных слов для обозначения состояний, действий или людей внутри группы.

• **Двойные послания и размытость правил.** Противоречивые требования создают когнитивный диссонанс и подавляют критическое мышление.

• **Культ вины.** Постоянный разбор ошибок с созданием ощущения никчёмности и зависимости от одобрения группы.

• **Эскалация заданий.** От безобидных (нарисовать символ, сделать фото) до тревожных (снять опасное действие, оставить надпись в общественном месте).

Уполномоченный при Президенте РФ по правам ребёнка выделяет следующие поведенческие маркеры вовлечения несовершеннолетнего в деструктивные онлайн-сообщества: резкие изменения в поведении (вспыльчивость, агрессивность или, наоборот, замкнутость), появление криминального сленга, интерес к контенту с насилием, скрытность в цифровой среде (пароли на устройствах, анонимные режимы), разрыв социальных связей со старыми друзьями и семьёй, появление новых знакомых, которых ребёнок не представляет родителям, специфический внешний вид (одежда, причёска, аксессуары с символикой деструктивных сообществ), обесценивание общечеловеческих норм.

6. Механизмы вовлечения в деструктивные сообщества

Механизмы вовлечения в деструктивные сообщества строятся на эксплуатации базовых психологических потребностей — потребности в принадлежности, признании, автономии и поиске смысла. Дети и подростки составляют особую группу риска вследствие возрастающей потребности в самоидентификации, подверженности эмоциональным воздействиям, склонности к подражательству, ограниченного жизненного опыта и незрелости оценочных способностей, а также поиска авторитета вне традиционной системы взрослых.

Факторы, повышающие вероятность вовлечения:

• низкий уровень образования и социальной адаптации;

• конфликты в семье, недостаточное внимание родителей;

• ощущение несправедливости и ущемления прав;

• наличие негативного опыта дискриминации;

• попадание в неблагополучную социальную среду.

Воронка вовлечения — маркетинговая модель рекрутинга, реализуемая в несколько этапов:

1. **Привлечение в нейтральную группу.** Пользователь попадает в группу по интересам (игры, музыка, аниме) через рекомендательные алгоритмы, репосты, приглашения от знакомых.

2. **Отбор по активности.** Кураторы анализируют поведение участников: частоту публикаций, готовность выполнять задания, эмоциональную вовлечённость. Наиболее активные приглашаются в более закрытые чаты.

3. **Перевод в закрытые каналы.** В закрытых группах постепенно, шаг за шагом, вводится деструктивный контент. Происходит сужение информационного поля, формирование «информационного пузыря».

4. **Вовлечение в противоправную деятельность.** На финальном этапе участнику предлагаются конкретные действия: от распространения материалов до совершения преступлений.

Основные техники манипулятивного воздействия:

• **Создание иллюзии заботы.** Куратор хвалит, поддерживает, проявляет интерес к проблемам.

• **Поляризация картины мира.** Разделение на «своих» и «чужих», формирование образа общего врага. Участников заставляют менять аватарки на одинаковые — знак «посвящения».

• **Геймификация.** Противоправные действия маскируются под «квесты» с этапами и «наградами».

• **Эмоциональная раскачка.** Последовательное усугубление эмоционального состояния жертвы с переходом к гиперконтролю, который реализуется под видом заботы.

• **Шантаж и угрозы.** Использование компромата, запугивание последствиями отказа.

• **Идеологическая обработка.** Подбрасывание тенденциозных материалов, игра на чувствах жалости или справедливости.

• **Создание искусственного дефицита.** Ощущение ограниченности времени или ресурсов побуждает к быстрому принятию решений без раздумий.

7. Вербовка, манипуляция, радикализация деструктива

Вербовка в смысле уголовного законодательства — это умышленные действия, направленные на вовлечение лица в совершение преступлений путём уговоров, подкупа, угрозы, убеждения, просьб, предложений. Статья 205.1 УК РФ устанавливает уголовную ответственность за вовлечение в совершение преступлений террористической направленности и за содействие террористической деятельности.

Стратегия противодействия экстремизму в Российской Федерации, утверждённая Указом Президента РФ от 28.12.2024 № 1124, констатирует, что экстремистские и иные антиобщественные организации используют информационно-телекоммуникационные сети, включая сеть «Интернет», мультимедийные и онлайн-технологии для вербовки новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии, а также финансирования экстремистской деятельности. Отмечаются попытки создания в различных регионах России законспирированных ячеек экстремистских и террористических организаций, в том числе осуществление вербовки новых участников, их обучение и подготовка террористов-одиночек дистанционным способом.

Стратегия определяет **радикализм** как приверженность идеологии насилия, характеризующуюся стремлением к решительному и кардинальному изменению основ конституционного строя Российской Федерации, нарушению единства и территориальной целостности. **Радикализация** — процесс, при котором лицо переходит от поддержки умеренных взглядов к поддержке крайних идеологических воззрений, часто связанных с насилием и экстремизмом. Этот процесс может происходить через интернет, социальные сети или личные контакты.

Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (в действующей редакции) определяет экстремистскую деятельность как включающую, среди прочего, возбуждение социальной, расовой, национальной или религиозной розни; пропаганду исключительности, превосходства либо неполноценности человека по признакам социальной, расовой, национальной, религиозной или языковой принадлежности; публичные призывы к осуществлению указанных деяний. Статья 12 закона прямо запрещает использование сетей связи общего

пользования и информационно-телекоммуникационных сетей, в том числе сети «Интернет», для осуществления экстремистской деятельности.

К числу типичных признаков радикализации несовершеннолетних относятся:

• резкое изменение круга общения, закрытость, замкнутость;

• уход от привычных хобби и увлечений;

• изменение манеры речи и лексикона, использование специфической терминологии;

• появление интереса к экстремистским материалам в сети;

• повышенная агрессивность, конфликты с окружающими.

Особую опасность представляет использование мессенджеров (в частности, Telegram), обеспечивающих высокую степень анонимности и защищённости переписки. Закрытые чаты и каналы с ограниченным доступом, боты для анонимной коммуникации, зашифрованные группы, применяющие стеганографию, а также фейковые сообщества по интересам, постепенно переключающиеся на радикальный контент, — всё это инструменты вербовки в цифровой среде.

8. Профилактика и противодействие вовлечению в деструктивные сообщества

Противодействие вовлечению в деструктивные сообщества требует комплексного подхода, объединяющего нормативно-правовое регулирование, психолого-педагогическую поддержку, технологические инструменты мониторинга и вовлечённость семьи и общества.

Нормативно-правовой уровень. Стратегия противодействия экстремизму (Указ № 1124 от 28.12.2024) определяет следующие направления государственной политики в информационной сфере: противодействие пропаганде идей экстремизма в сети «Интернет»; проведение мониторинга для выявления распространения экстремистской идеологии и принятие мер реагирования, включая ограничение доступа; проведение мероприятий по своевременному выявлению и пресечению фактов радикализации несовершеннолетних; недопущение вовлечения молодёжи в экстремистскую деятельность путём воспитания гражданственности, патриотизма и нравственности; повышение роли семьи в предупреждении радикализации.

Федеральный закон № 114-ФЗ от 25.07.2002 устанавливает, что противодействие экстремистской деятельности осуществляется по направлениям: принятие профилактических мер, направленных на предупреждение экстремистской деятельности, выявление и устранение причин и условий, способствующих её осуществлению; выявление, предупреждение и пресечение экстремистской деятельности.

Психолого-педагогический уровень. Профилактическая работа в образовательных организациях должна быть ориентирована на три результата: становление и развитие правового сознания; развитие устойчивости к негативным влияниям информационной среды; компетентность в сфере информационно-психологической безопасности — медиаграмотность, знание основ информационной безопасности, критическое мышление. Начинать работу целесообразно с младшего подросткового возраста (5–6 класс), постепенно формируя навыки критического мышления и готовность к противостоянию манипуляции.

Семейный уровень. Ключ к безопасности — не контроль любой ценой, а доверие. Регулярное обсуждение с ребёнком событий его онлайн- и офлайн-жизни, обсуждение механизмов работы вербовщиков, обучение ребёнка задавать вопросы: «Зачем мне это предлагают?», «Что человек получит от моего участия?», «Есть ли другие точки зрения?».

Индивидуальный уровень. При обнаружении признаков вовлечения необходимо:

1. Сохранить доказательства — скриншоты переписки, аудиозаписи.
2. Заблокировать подозрительный контакт или аккаунт.
3. Незамедлительно обратиться в правоохранительные органы.

4. При необходимости — обратиться за психологической помощью.

Технологический уровень. Внедрение систем искусственного интеллекта для выявления подозрительных паттернов общения, сотрудничество с владельцами платформ по удалению запрещённого контента, разработка приложений с функцией «тревожной кнопки» для сообщения об угрозах.

9. Правила коммуникации в цифровой среде

Концепция формирования и развития культуры информационной безопасности граждан определяет культуру информационной безопасности как совокупность сформированных знаний, умений и навыков, обеспечивающую безопасное пребывание гражданина в информационном пространстве. Стратегической целью государственной политики в этой области является формирование у граждан навыков противодействия угрозам информационной безопасности, в том числе информационно-психологическим.

На основе положений действующего законодательства и рекомендаций по цифровой гигиене формулируются следующие базовые правила коммуникации в цифровой среде:

Правило верификации собеседника. Не передавать личную информацию (адрес, место учёбы или работы, данные родственников, пароли, коды из SMS) незнакомым лицам. Проверять личность собеседника через независимые каналы связи. При получении сообщения от знакомого с необычной просьбой — перезванивать по известному номеру для подтверждения.

Правило информационной минимизации. Публиковать в открытом доступе только ту информацию, раскрытие которой не может нанести ущерб. Использовать настройки приватности для ограничения доступа к личным данным.

Правило критической оценки. Проверять источники информации, не доверять «слишком хорошим» предложениям, распознавать эмоциональные триггеры: если сообщение вызывает сильные эмоции (страх, вина, радость), это может быть признаком манипуляции.

Правило отказа от секретности. Отказываться от просьб хранить секреты от родителей или законных представителей. Фраза «только не рассказывай никому» — сигнал тревоги.

Правило ограничения реактивности. Не отвечать на провокации ответной провокацией. Не вступать в переписку с агрессорами. Признать «стоп» как внутренний сигнал к прекращению коммуникации при столкновении с подозрительным контентом.

Правило осознанного цифрового следа. Помнить, что любая размещённая в сети информация может быть сохранена, скопирована и использована против автора. Не пересылать интимные фотографии, не публиковать информацию о местоположении в реальном времени, не разглашать планы и маршруты.

Правило правовой осведомлённости. Знать, что распространение оскорблений, клеветы, угроз, экстремистских материалов, чужих персональных данных влечёт административную или уголовную ответственность. Проверять информацию на предмет наличия в перечне экстремистских материалов Минюста России перед её распространением.

Правило обращения за помощью. При столкновении с угрозой — сообщать о подозрительных предложениях взрослым, в правоохранительные органы, на платформы подачи жалоб (Роскомнадзор, администрация социальной сети). Не пытаться разрешить ситуацию самостоятельно.

10. Заключение

Опасности, связанные с коммуникацией в цифровой среде, носят системный многоуровневый характер и требуют адекватного системного противодействия. Нормативно-правовая база Российской Федерации включает Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон № 114-ФЗ «О противодействии экстремистской деятельности», Федеральный закон № 216-ФЗ о противодействии распространению деструктивного контента, Стратегию противодействия экстремизму (Указ Президента РФ от 28.12.2024 № 1124), Концепцию формирования и развития культуры информационной безопасности (распоряжение Правительства РФ от 22.12.2022 № 4088-р), а также соответствующие нормы УК РФ и КоАП РФ. Данная нормативная база устанавливает пределы допустимого поведения в цифровой среде, определяет санкции за правонарушения и задаёт стратегические ориентиры профилактической работы.

Однако правовое регулирование само по себе не может заменить индивидуальную ответственность. Ключевым фактором противодействия коммуникационным угрозам остаётся культура информационной безопасности гражданина — система знаний, умений и навыков, обеспечивающая безопасное пребывание в информационном пространстве. Формирование этой культуры составляет стратегическую цель государственной политики и должно осуществляться непрерывно, начиная с раннего возраста, с адаптацией под возрастные категории и с учётом специфики конкретных угроз.