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

ЛЕКЦИЯ 18. ТЕМА 1.18 ДОСТОВЕРНОСТЬ ИНФОРМАЦИИ В ЦИФРОВОЙ СРЕДЕ

1. Достоверность информации в цифровой среде: понятие и значение

Цифровая среда представляет собой совокупность информационно-телекоммуникационных сетей, систем и ресурсов, обеспечивающих создание, хранение, обработку и распространение информации в электронном виде. В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация определяется как сведения (сообщения, данные) независимо от формы их представления. Базовым принципом правового регулирования в данной сфере закреплена свобода поиска, получения, передачи, производства и распространения информации любым законным способом, а также установление ограничений доступа к информации только федеральными законами.

Достоверность информации — это свойство информации, отражающее объективное соответствие содержания информации реальному положению дел. В цифровой среде это понятие приобретает особую значимость по причине высокой скорости распространения данных, анонимности источников, а также возможности манипуляции с использованием технологий искусственного интеллекта. Достоверность следует отличать от точности (количественной характеристики) и полноты (исчерпывающего характера сведений). Достоверная информация одновременно должна быть актуальной и проверяемой.

Ключевая проблема цифровой среды заключается в том, что объём производимой и распространяемой информации превышает возможности индивидуальной верификации. Пользователь не располагает ресурсами для самостоятельной проверки каждого сообщения, что создаёт благоприятную почву для распространения недостоверных сведений, дезинформации и информационных манипуляций.

2. Источники информации. Проверка на достоверность

Источники информации в цифровой среде классифицируются по уровню доверия и институциональному статусу:

Официальные источники — государственные органы и органы местного самоуправления, публикующие информацию в установленном порядке. Доступ к информации о деятельности государственных органов закреплён как один из принципов правового регулирования в сфере информации. Официальные источники обладают наивысшим уровнем доверия, поскольку несут правовую ответственность за достоверность публикуемых сведений.

Редакционные источники — средства массовой информации, зарегистрированные в соответствии с Законом Российской Федерации от 27 декабря 1991 г. № 2124-I «О средствах массовой информации». Редакции несут ответственность за достоверность распространяемой информации и обязаны опровергать недостоверные сведения.

Пользовательский контент — информация, создаваемая и распространяемая пользователями социальных сетей, мессенджеров, блоговых платформ без редакционной обработки. Этот тип источников характеризуется наименьшим уровнем доверия, поскольку не проходит процедуру профессиональной проверки и не предполагает институциональной ответственности автора.

Агрегаторы — сервисы, автоматически собирающие и ранжирующие информацию из различных источников. Агрегаторы не создают собственный контент, но определяют его видимость для пользователя через алгоритмы ранжирования.

Проверка на достоверность включает следующие этапы:

1. **Идентификация источника** — установление автора, владельца ресурса, даты и места публикации. Проверка регистрации домена, истории аккаунта, наличия контактных данных редакции.

2. **Кросс-проверка** — сопоставление информации с сообщениями других источников, желательно независимых и разнотипных (официальные документы, репортажи разных агентств, экспертные заключения).

3. **Контекстная проверка** — установление полного контекста события, включая предшествующие и последующие обстоятельства, чтобы исключить искажение путём вырывания фактов из контекста.

4. **Проверка первоисточника** — отслеживание цепочки цитирования до первоначального источника. Часто недостоверная информация возникает в результате многократного перепубликования с постепенным искажением содержания.

5. **Экспертная оценка** — привлечение специалистов соответствующей предметной области для оценки правдоподобия утверждения с точки зрения фактических и научных данных.

3. «Информационный пузырь», манипуляция сознанием, пропаганда

Термин «информационный пузырь» (также «фильтрующий пузырь», «эхо-камера») обозначает состояние информационной изоляции пользователя, возникающее в результате работы алгоритмов персонализации интернет-сервисов — поисковых систем, социальных сетей, новостных агрегаторов, — которые подбирают контент на основе предыдущих предпочтений, поведения и демографических данных пользователя. Концепция введена американским исследователем Илаем Паризером в 2011 году. В таком пузыре пользователь получает преимущественно информацию, подтверждающую его существующие взгляды, и реже сталкивается с альтернативными точками зрения.

Научное различение «эхо-камер» и «эпистемических пузырей» проводится по характеру их формирования. Эхо-камеры — это фактически замкнутые коммуникативные пространства, образованные целенаправленными усилиями единомышленников, где взгляды, противоречащие принятой в сообществе позиции, намеренно дискредитируются и подавляются. Эпистемические пузыри и пузыри фильтров возникают спонтанно, в силу внешних факторов — недоступности определённых источников или действия алгоритмов персонализации.

В условиях эхо-камеры дезинформация, соответствующая взглядам аудитории, распространяется быстрее и легче, так как не встречает критического фильтра. Это формирует у пользователя искажённую картину мира, снижает способность к критическому восприятию информации и повышает уязвимость к манипуляциям.

Манипуляция сознанием в цифровой среде представляет собой целенаправленное воздействие на восприятие информации, при котором источник манипуляции скрывает свои истинные цели. К числу основных приёмов манипуляции относятся:

- **Подмена фактов мнениями** — представление субъективных суждений в форме фактических утверждений.
- **Эмоциональное заражение** — использование эмоционально окрашенной лексики, провоцирующей страх, гнев или возмущение, что снижает способность к рациональному анализу.
- **Селективный подбор фактов** — сообщение достоверной, но неполной информации, формирующей искажённое представление о событии.
- **Ложная дихотомия** — представление ситуации как выбора исключительно из двух взаимоисключающих вариантов.

Пропаганда в цифровой среде отличается от традиционных форм систематическим использованием алгоритмов распределения контента, таргетинга и автоматизированных сетей аккаунтов. Цифровая пропаганда характеризуется персонализацией воздействия — сообщение адаптируется под профиль конкретного пользователя на основе анализа его поведенческих данных.

4. Фальшивые аккаунты, вредные советчики, манипуляторы

Фальшивые аккаунты (боты, тролли, фиктивные профили) представляют собой инструмент целенаправленной дезинформации в цифровой среде. К основным типам относятся:

Сетевые боты — автоматизированные или полуавтоматизированные аккаунты, используемые для массового распространения сообщений, создания искусственного тренда, накрутки рейтингов и симуляции общественной поддержки. Боты способны генерировать тысячи публикаций в единицу времени, создавая иллюзию широкой общественной дискуссии.

Тролли — реальные лица, действующие от фальшивых аккаунтов с целью провокации конфликтов, распространения провокационного контента и дезорганизации конструктивной дискуссии. Троллинг может носить как индивидуальный, так и организованный характер.

Фиктивные профили — аккаунты, имитирующие реальных людей или организации для получения доступа к аудитории и доверия. Используются для сбора персональных данных, распространения дезинформации от имени авторитетных источников и проведения мошеннических схем.

Вредные советчики — аккаунты или ресурсы, позиционирующие себя как экспертные источники, но распространяющие непрофессиональные, некомпетентные или заведомо ложные рекомендации, особенно в сфере медицины, финансов, права и безопасности. Опасность вредных советчиков связана с тем, что их рекомендации могут привести к реальному ущербу для жизни, здоровья, имущества или прав пользователя.

В соответствии с действующим законодательством Российской Федерации организаторы распространения информации в сети «Интернет» обязаны идентифицировать пользователей и хранить соответствующие данные, что создаёт правовые предпосылки для противодействия анонимной дезинформации. Провайдер хостинга вправе осуществлять деятельность по предоставлению вычислительной мощности для размещения информации в сети «Интернет» только после прохождения идентификации и аутентификации лицами, обратившимися к провайдеру.

5. Понятие «фейк», цели и виды, распространение фейков

Фейк (от англ. fake — подделка) — это намеренно созданная и распространяемая ложная информация, представленная в форме достоверного сообщения. В российском законодательстве используется термин «заведомо недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений».

Цели распространения фейков:

- Политические — влияние на общественное мнение, дискредитация политических субъектов, формирование нужного отношения аудитории к событиям и процессам.
- Экономические — манипулирование рынком, снижение или повышение стоимости активов, нанесение репутационного ущерба конкурентам.
- Дестабилизирующие — провокация массовых нарушений общественного порядка, создание угрозы жизни и здоровью граждан, дезорганизация функционирования инфраструктуры.
- Вовлекающие — привлечение внимания аудитории с целью монетизации контента через рекламные показы.

Виды фейков:

1. **Фабрикация** — полностью вымышленная информация, не имеющая реального фактического основания.
2. **Манипуляция фактами** — использование реальных событий, но с искажением их смысла, контекста или масштаба.
3. **Атрибутивный фейк** — приписывание реальных высказываний или действий лицам, которые их не совершали.

4. **Визуальный фейк** — использование модифицированных, смонтированных или сгенерированных изображений и видео (дипфейки), представляемых как документальные.

5. **Контекстный фейк** — использование подлинного изображения или видео из другого события, времени или места с утверждением о его принадлежности к актуальному событию.

Распространение фейков в цифровой среде характеризуется эффектом каскадирования: одно сообщение может быть републиковано тысячи раз за короткий промежуток времени. Алгоритмы рекомендательных систем социальных платформ способствуют ускоренному распространению контента, вызывающего сильную эмоциональную реакцию, что делает провокационные и сенсационные фейки особенно вирусоспособными.

6. Правила и инструменты для распознавания фейковых текстов и изображений

Правила распознавания фейковых текстов:

1. **Анализ источника** — проверка авторства, даты публикации, доменного имени. Отсутствие указания на конкретный источник первичной информации — существенный индикатор недостоверности.

2. **Проверка логической структуры** — выявление противоречий внутри текста, утверждений, не следующих из приведённых фактов, необоснованных обобщений.

3. **Стилистический анализ** — наличие эмоционально-окрашенной лексики, не свойственной информационным материалам, избыточное использование восклицательных знаков, заголовков-кликбейтов.

4. **Кросс-проверка** — поиск той же информации в других источниках. Если сообщение публикуется только в одном источнике ненадлежащего уровня, это требует дополнительной проверки.

5. **Проверка дат** — соответствие даты публикации описываемым событиям. Часто используются устаревшие материалы, которые подаются как актуальные.

Инструменты распознавания фейковых изображений:

1. **Обратный поиск по изображению** — технологии, позволяющие найти исходный источник изображения и его предыдущие публикации (Google Images, Яндекс.Картинки, TinEye).

2. **Анализ метаданных** — проверка данных EXIF, содержащих информацию о дате и времени создания файла, модели камеры, координатах съёмки.

3. **Выявление артефактов монтажа** — анализ на наличие неестественных границ объектов, расхождений в освещении, несоответствий пропорций, следов клонирования участков изображения.

4. **Распознавание дипфейков** — выявление признаков синтезированного видео: микровыражений лица, не соответствующих эмоциональному контексту, артефактов на границах лица и шеи, неестественного мигания, расхождий между движением губ и звуковым рядом.

7. Понятие прав человека в цифровой среде, их защита

Права человека в цифровой среде представляют собой распространение и адаптацию традиционных прав и свобод на условия информационного общества. Конституционная основа цифровых прав закреплена в статьях 23 и 24 Конституции Российской Федерации. Статья 23 гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, защиту чести и доброго имени, а также право на тайну переписки, телефонных переговоров и иных сообщений. Статья 24 устанавливает запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. Ограничение права на тайну переписки и сообщений допускается только на основании судебного решения.

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

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» создаёт правовую основу обращения с персональными данными в целях реализации конституционных прав человека, в том числе права на неприкосновенность частной жизни и личную тайну. Закон устанавливает принципы и условия обработки персональных данных, определяет права субъектов персональных данных и обязанности операторов. Обработка специальных категорий персональных данных — сведений о расовой и национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни — не допускается, за исключением прямо предусмотренных случаев.

Ключевыми правами человека в цифровой среде являются:

- **Право на доступ к информации** — закреплено в статье 8 Федерального закона № 149-ФЗ и включает право искать, получать, передавать и распространять информацию законным способом.
- **Право на неприкосновенность частной цифровой жизни** — защита от несанкционированного сбора, обработки и распространения персональных данных.
- **Право на тайну коммуникаций** — гарантия конфиденциальности переписки в мессенджерах и электронной почте.
- **Право на защиту от вредной информации** — гарантированное Федеральным законом от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» право на безопасную информационную среду.
- **Право на свободу выражения мнений в цифровой среде** — реализация конституционного права на свободу мысли и слова с использованием цифровых коммуникаций.

На международном уровне ЮНЕСКО разработаны «Руководящие принципы регулирования цифровых платформ», в которых изложены обязанности государств, цифровых платформ и гражданского общества по обеспечению свободы выражения мнений и доступа к информации. В Руководящих принципах определены три основных направления деятельности: обеспечение жизнеспособности СМИ, прозрачности платформ и развитие критического мышления пользователей.

8. Ответственность за действия в Интернете. Запрещённый контент

Правовая ответственность в информационной сфере регламентируется нормами административного, уголовного и гражданского права. Законодательство устанавливает ответственность за различные виды правонарушений, совершаемых с использованием сети «Интернет».

Ответственность за распространение недостоверной информации. Федеральным законом от 18 марта 2019 г. № 31-ФЗ внесены изменения в статью 15.3 Федерального закона № 149-ФЗ, устанавливающие механизм ограничения распространения недостоверной общественно значимой информации, создавшей угрозу причинения вреда жизни и здоровью граждан, имуществу, общественному порядку и безопасности, а также угрозу нарушения функционирования объектов жизнеобеспечения и инфраструктуры. Генеральный прокурор Российской Федерации или его заместители направляют обращение в Роскомнадзор, который уведомляет редакцию сетевого издания о необходимости удаления недостоверной информации. При невыполнении требования Роскомнадзор направляет операторам связи требование об ограничении доступа к ресурсу.

В Кодексе Российской Федерации об административных правонарушениях (статья 13.15) установлена ответственность за распространение заведомо недостоверной общественно значимой информации под видом достоверных сообщений. Штрафы для граждан составляют от 30 000 до 100 000 рублей; при наступлении последствий в виде нарушения функционирования инфраструктуры — от 100 000 до 300 000 рублей; при

причинении вреда жизни, здоровью или имуществу, массовых нарушениях общественного порядка — от 300 000 до 400 000 рублей.

Уголовная ответственность за фейки. Статья 207.3 Уголовного кодекса Российской Федерации устанавливает уголовную ответственность за публичное распространение под видом достоверных сообщений заведомо ложной информации об использовании Вооружённых Сил Российской Федерации, исполнении государственными органами своих полномочий за пределами территории Российской Федерации, а также об оказании добровольческими формированиями содействия в выполнении задач, возложенных на Вооружённые Силы. Базовый состав предусматривает наказание в виде штрафа от 700 000 до 1 500 000 рублей либо лишения свободы на срок до пяти лет. При совершении деяния с использованием служебного положения, группой лиц, из корыстных побуждений или по мотивам ненависти размер штрафа увеличивается до 3 000 000 — 5 000 000 рублей, а срок лишения свободы — до десяти лет. При наступлении тяжких последствий наказание составляет лишение свободы на срок от десяти до пятнадцати лет.

Федеральным законом от 14 февраля 2024 г. № 11-ФЗ расширен перечень преступлений, за которые может предусматриваться конфискация имущества. Конфискации подлежат денежные средства, ценности или иное имущество, полученные в результате совершения преступления по статье 207.3 УК РФ, при условии совершения деяния из корыстных побуждений.

Запрещённый контент. В соответствии с Федеральным законом от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» запрещается использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», для осуществления экстремистской деятельности. Экстремистские материалы определяются как предназначенные для распространения документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость её осуществления. В федеральный перечень экстремистских материалов, ведущийся Минюстом России, к концу 2025 года входило около 5 500 наименований.

Федеральным законом от 22 июля 2025 г. № 281-ФЗ введена административная ответственность за умышленный поиск заведомо экстремистских материалов и получение к ним доступа, в том числе с использованием программно-аппаратных средств (VPN-сервисов). Штраф для граждан составляет от 3 000 до 5 000 рублей. Ответственность наступает только при доказанном умысле — случайный доступ к запрещённым материалам правонарушением не признаётся. Этот же закон установил ответственность за рекламу средств обхода блокировок: штраф для граждан — от 50 000 до 80 000 рублей, для юридических лиц — от 200 000 до 500 000 рублей.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» запрещает распространение среди детей информации, побуждающей к совершению действий, представляющих угрозу жизни и здоровью, способной вызвать желание употреблять наркотические средства, алкоголь и табачные изделия, оправдывающей насилие и жестокость, содержащей изображение сексуального насилия, оскорбляющей человеческое достоинство. Информационная продукция классифицируется по возрастным категориям: 0+, 6+, 12+, 16+ и 18+.

9. Защита прав в цифровом пространстве

Защита прав человека в цифровом пространстве реализуется через систему правовых, организационных и технических мер.

Правовые механизмы защиты включают возможность обращения в суд за защитой нарушенных прав, в том числе права на неприкосновенность частной жизни и защиту персональных данных. Субъект персональных данных вправе требовать возмещения убытков и компенсации морального вреда в судебном порядке. Федеральный орган исполнительной власти, осуществляющий контроль и надзор в сфере

информационных технологий и связи, вправе проводить проверку информационных систем обработки персональных данных, предъявлять требования по блокированию и удалению недостоверных или полученных незаконным путём персональных данных, устанавливать запрет на их обработку.

Организационные меры включают обязанности организаторов распространения информации в сети «Интернет» по выявлению и блокировке противоправного контента. Социальные сети, включённые в реестр Роскомнадзора, обязаны иметь форму обратной связи для приёма жалоб пользователей на запрещённую информацию. За несоблюдение норм о самоконтроле предусмотрены штрафы до 8 000 000 рублей.

Технические меры включают применение средств защиты персональных данных от несанкционированного доступа, шифрование коммуникаций, использование систем фильтрации контента, а также программно-аппаратные средства защиты детей от информации, причиняющей вред их здоровью и развитию.

Деятельность по противодействию экстремистской деятельности в цифровой среде основывается на принципах приоритета обеспечения безопасности Российской Федерации, приоритета профилактических мер, сотрудничества государства с общественными объединениями и гражданами, а также неотвратимости наказания. Профилактические меры направлены на выявление и устранение причин и условий, способствующих осуществлению экстремистской деятельности.

В условиях стремительного развития цифровых технологий и появления новых форм информационных угроз ключевое значение приобретает формирование медиа- и информационной грамотности. Развитие критического мышления пользователей, способность к самостоятельной оценке достоверности информации и осознание правовых последствий действий в цифровой среде являются фундаментальными элементами информационной безопасности личности и государства.