МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.П. АСТАФЬЕВА
(КГПУ им. В.П. Астафьева)

Факультет: исторический
Выпускающая кафедра: философии, экономики и права

Амосова Яна Дмитриевна

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТНХНОЛОГИЙ КАК ИСТОЧНИК ПРОСВЕЩЕНИЯ ПОДРОСТКОВ

Направление подготовки: 44.03.05: педагогическое образование (с двумя профилями подготовки)
Направленность (профиль) образовательной программы: История и право

ДОПУСКАЮ К ЗАЩИТЕ
и.о. зав. кафедрой философии, экономики и права:
к. ф. н., доцент Лисина Лариса Георгиевна
_____
(дата, подпись)
Научный руководитель:
к. ф. н., доцент Лисина Лариса Георгиевна
_____
(дата, подпись)
Обучающийся: Амосова Яна Дмитриевна
_____
(дата, подпись)
Дата защиты_____
Оценка_____

Красноярск 2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современных условиях цифровой трансформации всех сфер общественной жизни возникает противоречие: наиболее действенные методы противодействия новым вызовам зачастую кроются не в сугубо технологических или карательных мерах, а в превентивном формировании правового сознания. Истоки эффективной защиты от киберугроз следует искать не столько в кодексах и нормативных актах, сколько в образовательном пространстве, где у будущих взрослых граждан закладываются основы понимания права и его роли в социуме.

Преступления в цифровой среде характеризуются сегодня беспрецедентной динамикой и масштабом. Преступления в сфере информационных технологий, понимаемые как общественно опасные деяния, посягающие на информационную безопасность, конфиденциальность, целостность и доступность данных, а также на права и законные интересе в интернете, представляют собой одну из наиболее значимых угроз как национальной, так и личной безопасности каждого гражданина в Российской Федерации. Их особая опасность обусловлена транснациональным характером, высокой адаптивностью и постоянно эволюционирующим инструментарием.

Сложившаяся практика противодействия данным противоправным деяниям традиционно акцентирует внимание на совершенствовании уголовно-правовых норм, развитии специализированных подразделений правоохранительных органов и внедрении сложных технических средств защиты. Бесспорно, эти элементы образуют необходимый каркас государственной политики в данной области. Однако, с нашей точки зрения, стратегическим и системообразующим фактором долгосрочной эффективности является формирование программы правового просвещения в области информационной безопасности на уровне школьного образования. Именно уроки обществознания, выполняющие не только просветительскую,

но и воспитательную функцию, выступают в качестве ключевого элемента профилактики киберпреступности. В рамках этих дисциплин закладывается фундамент правосознания, развиваются навыки критической оценки информации и формируется модель социально ответственного поведения в глобальном информационном пространстве, что в своей совокупности составляет основу цифровой грамотности гражданина Российской Федерации XXI века.

Актуальность исследования.

Мы рассматриваем школьный курс обществознания в качестве ключевого элемента в формировании правового просвещения и базовых компетенций, необходимых для безопасного и ответственного функционирования личности в цифровом пространстве. В текущий исторический момент, характеризующийся стремительной цифровизацией всех сфер жизни и одновременным ростом киберугроз, проблема противодействия преступлениям в сфере информационных технологий приобретает характер одной из доминирующих в повестке национальной безопасности. В связи с этим крайне важно уделить внимание не только развитию технических средств защиты или ужесточению репрессивных мер в отношении правонарушителей, но и системному правовому воспитанию, начинающемуся на этапе школьного образования. Поскольку если не заложить у школьников прочного фундамента правовых знаний и этических принципов поведения в сети, то впоследствии, сколь бы совершенным ни было законодательство и работа правоохранительных органов, полностью избавиться от последствий данной проблемы не представится возможным. Это обусловлено тем, что базовые модели правомерного поведения, критическое восприятия информации и осознание юридических последствий своих действий не были усвоены на начальном этапе социализации в сети «Интернет», что затрудняет не только адаптацию человека к требованиям цифрового сообщества, но и подрывает саму возможность построения

надежной системы кибербезопасности, основанной на гражданской ответственности. Именно поэтому в современных условиях необходимо начинать с формирования этой первоосновы – целенаправленного правового просвещения в школе, которое станет залогом осознанного соблюдения закона в цифровой среде на протяжении всей последующей жизни человека.

Объект исследования – преступления в сфере информационных технологий и меры по их предотвращению.

Предмет исследования – содержание и особенности ИТ-преступлений, а также просветительская деятельность в школе, связанная с их предотвращением.

Цель исследования – определить наиболее эффективные формы работы со школьниками в рамках просвещениях об угрозах и кибербезопасности.

Задачи исследования:

– Изучить документы нормативно-правовой базы о информационных преступлениях;

– Апробировать существующие форматы просвещения в школе;

– Оценить эффективность апробации в школе для определения наиболее результативного способа просвещения молодежи.

Источниковая база исследования.

Наше исследование опиралось на нормативно-правовые акты и законы в сфере регулирования информационных технологий, а также результаты апробации в общеобразовательных учреждениях, полученных в рамках интеграции методических разработок в учебный процесс на производственной педагогической практике.

Методологическая основа исследования.

Среди использованных нами методов стоит отметить методы познания, диалектический метод, метод системного анализ, логический метод, педагогический эксперимент и др.

Практическая значимость исследования.

Результаты исследования могут быть применены на уроках обществознания в средней и старшей школе при изучении блока «Правовое регулирование общественных отношений», а также в рамках внеурочной и проектной деятельности.

Структура работы.

Выпускная квалификационная работа состоит из введения, 2 глав, заключения, списка источников и литературы, а также приложений.

ГЛАВА 1. ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИ

1.1. Понятие, виды и характеристика преступлений в сфере информационных технологий

В условиях тотальной цифровизации, когда информационно-телекоммуникационные сети стали неотъемлемой средой для коммуникации, образования, бизнеса и управления, возникает принципиально новая область социальных рисков. Противоречие между безграничными возможностями технологий и уязвимость созданных на их основе общественных отношений порождает феномен преступности, которая использует технологии в качестве как инструмента, так и среды совершения новых противоправных деяний. Понимание сущности, разновидностей и отличительных черт преступлений в сфере информационных технологий (IT, оно же ИТ) составляет фундаментальную основу для разработок педагогических стратегий профилактики рискованного поведения в интернете.

В научной литературе и правоприменительной практике используются различные термины для обозначения противоправных деяний, связанных с цифровой средой: «компьютерные преступления», «киберпреступность», «преступления в сфере компьютерной информации», «IT-преступления». Эти понятия часто пересекаются, но имеют смысловые нюансы.[1] Наиболее узким и строго формализованным в российском законодательстве является термин «преступление в сфере компьютерной информации». Он закреплен в главе 28 Уголовного кодекса Российской Федерации (УК РФ) и охватывает деяния, непосредственным объектом которых выступают общественные отношения, обеспечивающие безопасность производства, хранения, использования или распространения информации, обрабатываемой с помощью электронно-вычислительной техники.[2] Согласно разъяснениям правоохранительных органов, к таким преступлениям относятся неправомерный доступ к компьютерной информации (ст. 272 УК РФ),[3] создание, использование и

распространение вредоносных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и сетей (ст. 274 УК РФ),[4] а также ряд других составов, введенных в последние годы для противодействия угрозам критической информационной структуре (ст. 274.1 УК РФ).

Более широким является понятие «преступления в сфере информационных технологий» (IT-преступления). Оно включает не только «чисто» компьютерные преступления по главе 28 УК РФ, но и любые другие общественно-опасные деяния, совершаемые с использованием IT-средств, где компьютер или сеть выступают ключевым инструментом для достижения преступного результата. К этой категории можно отнести мошенничество с использованием электронно-платежных средств (ст. 159.6 УК РФ), незаконный оборот средств платежей (ст.187 УК РФ), распространение порнографических материалов (ст. 242 УК РФ), клевету (ст. 128.1 УК РФ), угрозу убийством (ст. 119 УК РФ) и многие другие составы, объективная сторона которых реализуется через интернет-среду. Родовое понятие «ИТ-преступления» охватывает как преступления против информационной безопасности сами по себе, так и традиционные преступления, модифицированные включением в их состав цифровой среды.

С точки зрения педагогического исследования, важным является также криминологическое понятие «киберпреступность», которое акцентирует внимание на совокупности таких деяний как на социальном явлении, характеризующемся специфическими причинами, условиями, личностными особенностями преступников и высоким уровнем латентности. Именно такой подход позволяет рассматривать ИТ-преступность не просто как набор статей УК РФ, а как комплексную проблему, требующую, помимо правовых, также воспитательных и просветительских мер воздействия.

Классификация ИТ-преступлений возможна по различным основаниям: по непосредственному объекту посягательства, по способу совершения, по цели деяния, по субъективным характеристикам преступника.[5] Для целей

правового просвещения наиболее наглядной и содержательной является классификация, сочетающая юридический (нормативный) и криминологический (феноменологический) подходы:

1. Преступления, непосредственно посягающие на информационную безопасность (глава 28 УК РФ). Это ядро ИТ-преступности, которое законодатель выделил в отдельную главу.

a. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Предметом этого преступления является охраняемая законом компьютерная информация – сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Суть деяния заключается в получении возможности знакомиться с такой информацией или использовать ее без правомерных оснований, если это повлекло ее уничтожение, блокирование, модификацию, копирование или нарушение работы ЭВМ, системы, сети.[6]

b. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). Данный состав направлен против целостности и функционирования компьютерных систем. Под вредоносной программой понимается программа (или ее модификации), заведомо приводящая к несанкционированному уничтожению, блокированию, модификации, копированию информации или нарушению работы ЭВМ. Сюда относятся не только классические вирусы и «черви», но и троянские программы, шпионское программное обеспечение (англ. «spyware»), программы-шифровальщики (англ. «ransomware»), ботнеты. Распространение может осуществляться через интернет-ресурсы, электронную почту, зараженные съемные носители.

c. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Субъектом этого преступления является лицо, имеющее правомерный доступ к ЭВМ или сети, но нарушившее установленные правила их эксплуатации, что повлекло

уничтожение, блокирование или модификацию охраняемой информации и причинило существенный вред. Это преступление часто связано с халатностью, небрежностью или недостаточной квалификацией администраторов систем.

d. Преступления против критической информационной инфраструктуры (КИИ) (ст.274.1 УК РФ и др.). Относительно новые составы, введенные для защиты объектов, нарушение функционирования которых может нанести ущерб национальной безопасности, экономике, здоровью населения. К ним относится неправомерное воздействие на КИИ, создание или использование вредоносных программ для КИИ.

2. Преступления против собственности, совершаемые с использованием ИТ.[7] Эта группа составляет значительную долю от всей киберпреступности и причиняет по-настоящему колоссальный материальный ущерб.

a. Компьютерное мошенничество (ст. 159.6 УК РФ). Хищение чужого имущества или приобретение права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи информации. Сюда относятся мошеннические «схемы» с использованием фишинговых сайтов, взлом аккаунтов пользователей в системах онлайн-банкинга, мошенничества на интернет-аукционах.

b. Кардинг (как часть мошенничества или ст. 187 УК РФ). Несанкционированные операции с различными реквизитами платежных карт (номер, срок действия, CVV-код), полученными путем взлома баз данных онлайн-магазинов, использования скимминговых устройств или вредоносного ПО.

c. Вымогательство (ст.163 УК РФ) в форме кибератак. Наиболее распространенный вид – атаки типа «отказ в обслуживании» (англ. «DDoS») с последующим требованием выкупа за прекращение атаки, а также

использование ransomware, который шифрует данные жертвы с требованием оплаты за получение доступа к ключу дешифрования[8].

3. Преступления против личности и общественной нравственности, совершаемые в цифровой среде.

a. Кибersталкинг (преследование в цифровой среде) и кибербуллинг (травля в цифровой среде).[9] Могут попадать под составы угрозы убийством или причинения тяжкого вреда здоровью (ст. 119 УК РФ), клеветы (ст. 128.1 УК РФ), оскорбления (ст. 5.61 КоАП РФ).[10] Постоянные унизительные сообщения, создание ложных профилей, публикация компрометирующих материалов – все это формы цифрового насилия, наносящего тяжелый психологический вред личности потерпевшего и, в том числе, самого преступника, особенно это актуально для подростковой среды, к примеру, в школе.

b. Распространение запрещенного контента. К этой категории относится оборот детской порнографии (ст. 242.1, 242.2 УК РФ), материалов, пропагандирующих экстремизм и терроризм (ст. 205.2, 280, 282 УК РФ), а также иной информации, распространение которой ограничено российским законодательством, например, о способах совершения самоубийства.

c. Торговля людьми в киберсексуальной эксплуатации. Жертв принуждают к трансляции действий сексуального характера через интернет в реальном времени. Для вербовки и контроля преступники активно используют социальные сети и мессенджеры.

4. Преступления против информационной безопасности и конституционного строя.

a. Кибертерроризм. Использование киберпространства для проведения атак на критически важные объекты (энергосистемы, транспорт, системы управления) с целью дестабилизации общества, запугивания населения или оказания давления на власти.[11] Такие деяния могут квалифицироваться по статьям о терроризме (ст. 205, 205.1 УК РФ) или диверсии (ст. 281 УК РФ).

b. Распространение ложной информации об общественно значимых событиях (фейки), создающее угрозу общественной безопасности (ст. 207.1, 207.2 УК РФ).

Современная ИТ-преступность обладает рядом отличительных признаков, которые обуславливают ее высокую общественную опасность и сложность противодействия.[12] Во-первых, это транснациональный характер – преступник, жертва, сервера с данными и средства платежа могут находиться в разных странах, что создает преодолеваемые, но крайне мешающие обстоятельства для юрисдикции, расследования и привлечения преступников к ответственности. Уоррен Баффет подчеркнул, что киберпреступность является «проблемой номер один для человечества» и представляет реальные угрозы для человечества. Во-вторых, это высокая степень анонимности и латентности – использование технологий шифрования, анонимных сетей, VPN-сервисов, криптовалют для расчетов позволяют преступникам эффективно скрывать свою личность в интернете.[13] Многие жертвы, особенно физические лица, не обращаются в правоохранительные органы из-за неверия в результативность, стыда или незнания процедуры. В-третьих – это динамичность и адаптивность. Инструментарий и методы киберпреступников эволюционируют быстрее, чем обновляется законодательство и разрабатываются подходящие меры защиты.

Появление новых технологий мгновенно порождает новые векторы атак. В-четвертых, это технологическая сложность и профессионализация[14] – для совершения расследования многих ИТ-преступлений требуются специальные глубокие знания.[15] Это привело к разделению труда в преступной среде: выявлялись специалисты по поиску уязвимостей, написанию вредоносного кода, организации фишинговых ссылок, «отмыванию» криптовалют. В этих обстоятельствах все еще наблюдается сохранение скрытности низкого уровня раскрываемости таких преступлений.[16] В-пятых, это массовый характер и масштабируемость – одна успешно разработанная вредоносная программа или фишинговая схема может почти мгновенно поразить миллионы устройств и

пользователей по всему миру, причинив колоссальный совокупный ущерб. Последняя характеристика – особенности субъектов преступлений. В сферу ИТ-преступлений активно вовлекаются молодые люди, включающие несовершеннолетних. Это часто связано не с корыстными мотивами в чистом виде, а с желанием самоутвердиться, продемонстрировать технические навыки друзьям, получить признание в своей субкультуре и прочее. Такая мотивация является важным объектом для педагогического воздействия и профилактики деструктивного поведения.

Преступления в сфере информационных технологий представляют собой сложный, многогранный феномен, охватывающий как специальные составы, направленные на защиту информационной безопасности, так и традиционные виды преступной деятельности, перенесенные в цифровую среду. Их систематизация и детальная характеристика позволяют не только в мелочах идентифицировать угрозы, но и выявить те узловые точки, где правовое регулирование и правоохранительная деятельность сталкиваются с наибольшими вызовами. Для педагогической науки и практики, на которых фокусируется данное исследование, это понимание является отправной точкой. Оно позволяет перейти от абстрактного осознания «киберугроз» к конкретному анализу тех поведенческих моделей, правовых дефицитов и этических лакун в сознании подростков, которые могут сделать их либо жертвами или участниками ИТ-преступлений.

1.2. Уголовно-правовая характеристика и ответственность за преступления в сфере IT по российскому законодательству

Правовое регулирование отношений в информационной среде и противодействие злоупотреблениям в ней представляют собой сложную систему норм различной отраслевой принадлежности и юридической силы. Его иерархическую основу образует Конституция Российской Федерации, которые задает фундаментальные векторы для законодательства. Статья 23

гарантирует право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, что напрямую коррелирует с защитой персональных данных и приватности в сети. Статья 29 провозглашает свободу мысли, слова, а также право свободно искать, получать, передавать, провозить и распространять информацию любым законным способом. Однако эта же статья устанавливает и конституционные основания для введения ограничений: в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Именно эти ограничительные уточнения являются правовой основой для криминализации многих деяний в ИТ-сфере, таких как распространение экстремистских материалов или детской порнографии в интернете.

Следующий уровень образуют кодифицированные акты и федеральные законы, формирующие отраслевой ландшафт. Ключевым среди них является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».[17] Он выполняет роль рамочного акта, закрепляющего основные понятия – информация, информационные технологии, информационная система, обладатель информации – а также принципы правового регулирования, в частности, принцип установления ограничения доступа к информации только федеральными законами, и основы режима информации, который может быть общедоступным или ограниченным в доступе. Этот закон служит отправной точкой для понимания того, что является охраняемым благом в цифровом пространстве.

Специализированное регулирование осуществляют законы, устанавливающие правовые режимы для конкретных видов информации:

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[18] детально регламентирует обработку любых сведений, прямо или

косвенно относящихся к физическому лицу, вводя жесткие требования к согласию субъекта, целям обработки, мерам безопасности и передаче. Нарушения могут повлечь как административную (ст. 13.11 КоАП РФ), так и уголовную ответственность.

2. Федеральные законы «О государственной тайне» и «О коммерческой тайне» защищают информацию, составляющую соответствующий вид тайны, устанавливая процедуры засекречивания, допуска и ответственности за разглашение этой информации.

3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»[19] легитимизирует использование электронных аналогов собственноручной подписи, обеспечивая юридическую значимость сделок и документов в электронной форме, что критически важно для развития государственных технологий и социальных отношений.

Трудовой кодекс (ТК РФ)[20] и Кодекс об административных правонарушениях (КоАП РФ) играют важную роль в системе правовой охраны. Трудовой кодекс РФ (глава 14) закрепляет особый режим обработки персональных данных сотрудника. КоАП РФ (глава 13) содержит широкий спектр составов административных правонарушений в области связи и информации: от нарушения порядка изготовления или распространения информационной продукции (ст. 13.21) до пропаганды наркотических средств в интернете (ст. 6.13) и неустранения администратором сайта запрещенной информации (ст. 13.41) Административная ответственность часто служит «первым рубежом» противодействия менее общественно опасным преступления в ИТ-сфере.

Центральное место в системе репрессивных мер занимает Уголовный кодекс РФ. Его глава 28 «Преступления в сфере компьютерной информации» содержит «специальные» составы, в которых компьютерная информация или средства ее обработки являются непосредственным объектом преступного посягательства.

В первую очередь, выделяет неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Объективная сторона заключается в преодолении средств защиты и получении возможности ознакомиться с информацией или работать с ней. Важным условием уголовной ответственности по базовой части статьи является наступление одного из последствий: уничтожение, блокирование, модификация, копирование информации либо нарушение работы ЭВМ, системы, сети. Это означает, что сам факт взлома пароля для просмотра данных, не повлекший указанных последствий, может остаться за рамками этой статьи, но может подпадать под иные нормы, например, нарушение тайны личной переписки – ст. 138 УК РФ. Квалифицированные составы (ч. 2, 3) вводят отягчающие признаки: совершение группой лиц по предварительному сговору или организованной группой; корыстная заинтересованность; причинение крупного ущерба свыше 1 млн. руб. или тяжких последствий. Санкции варьируются от штрафа до лишения свободы на срок до 7 лет.

Создание, распространение и использование вредоносных компьютерных программ – ст. 273 УК РФ. Данная статья криминализирует действия с программами или их модификациями, заведомо предназначенными для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты. Ключевым выступает умысел создателя или распространителя. Само по себе создание такого ПО, даже без его последующего использования, уже образует оконченное преступление. Часть 2 статьи ужесточает ответственность за те же деяния, повлекшие по неосторожности тяжкие последствия – дестабилизация работы критической инфраструктуры, причинение смерти человеку и подобное, предусматривая лишение свободы до 10 лет. В 2022 в статью были внесены существенные дополнения – ст. 273.1, 273.2 УК РФ, криминализирующие создание и использование специальных технических устройств (СТС), предназначенных для тайного получения информации с

технических каналов связи, например, для перехвата SMS или обхода 2FA, а также их сбыт.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей – ст. 274 УК РФ. Специфика этого состава в специальном субъекте – лицо, имеющее правомерный доступ к ЭВМ или сети и обязанное соблюдать правила их эксплуатации. Преступление совершается путем бездействия или небрежного действия. Ответственность наступает при условии причинения тяжких последствий (ч. 2) либо существенного вреда, который, как правило, трактуется оценочно, с учетом реального ущерба и упущенной выгоды.

Преступления против критической информационной структуры Российской Федерации (КИИ РФ) – ст. 274.1, 274.2 УК РФ. Это относительно новые нормы, введенные в 2017 году, отражают повышенную общественную опасность атак на объекты , обеспечивающие устойчивое функционирование ключевых отраслей экономики, государства и общества. Статья 274.1 УК РФ предусматривает ответственность за неправомерное воздействие на КИИ, а статья 274.2 – за создание использование и распространение вредоносных программ для КИИ. Санкции исключительно суровы – до 10 лет лишения свободы, а при наступлении тяжких последствий – до 15 лет.

Помимо главы 28, множество смежных составов в других главах УК РФ используются для квалификации ИТ-преступлений, где технология выступает инструментом:

1. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Специальная норма, охватывающая хищение денежных средств или прав на них путем вмешательства в функционирование информационных систем – взлом личного кабинета, модификация баз данных о балансе.

2. Незаконные организация и проведение азартных игр (ст. 171.2 УК РФ) и легализация денежных средств (ст. 174, 174.1 УК РФ). Онлайн-казино и обналичивание криптовалют, полученных преступных путем, являются типичными сферами применения данных статей.

3. Преступления против личности: клевета (ст. 128.1 УК РФ), оскорбление (ст. 5.61 КоАП РФ, а в отношении военнослужащих – ст. 336 УК РФ), угроза убийством (ст. 119 УК РФ), совершаемые публично в сети.

4. Преступления против общественной безопасности и государственной власти: публичные призывы к экстремизму или терроризму (ст. 205.2, 280 УК РФ), возбуждение ненависти либо вражды (ст. 282 УК РФ), распространение заведомо ложной общественно значимой информации (ст. 207.1, 207.2, 207.3 УК РФ).

Статистические данные, предоставленные МВД России, ярко иллюстрируют масштаб и динамику проблемы.[21] В 2022 году было зарегистрировано 522 тыс. преступлений и использованием ИТ-технологий, что составило 26,5% от общего числа зарегистрированных преступлений. Рост в январе-марте 2023 года на 22,7% по сравнению с аналогичным периодом прошлого года свидетельствует о экспоненциальном характере угрозы. Распределение по каналам совершения: интернет (115,3 тыс.), телефон (66,1 тыс.), использование банковских карт (30,4 тыс.) – демонстрирует основные векторы атак.

Особую тревогу вызывает структура преступности: более половины (52,1%) киберпреступлений относится к категории тяжких и особо тяжких. Однако уровень раскрываемости этих деяний остается низким – около 42,3%. Этот разрыв между регистрацией и раскрытием указывает на основные проблемы сформированной системы.

В связи с этим, как показывает практика, упор лишь на карательные меры не может кардинально изменить ситуацию.[22] Эффективное противодействие требует комплексного подхода, где уголовное

преследование является последним, а не единственным звеном. Система должна включать в себя техническую защиту, административное регулирование, финансовый мониторинг и, что наиболее значимо для долгосрочной перспективы, всеобъемлющее правовое просвещения среди населения.

Российское законодательство в области противодействия ИТ-преступлениям представляет собой разветвленную и динамично развивающуюся систему, интегрирующую конституционные принципы, отраслевое законодательство, административные и уголовно-правовые запреты. Уголовный кодекс, сосредоточив в главе 28 «ядро» компьютерных преступлений, дополняет его широким спектром смежных составов, позволяющих квалифицировать практически любое общественно опасное деяние, совершенное с использованием цифровых технологий. Однако анализ статистики и практики раскрытия указывает на значительные трудности в реализации этих правовых норм. Это не умаляет значения уголовной ответственности как главного правового барьера,[23] но со всей очевидностью указывает на то, что стратегический ресурс снижения таких преступлений лежит в области упреждающего правового просвещения среди населения. Понимание подростками не только статей УК РФ, но и логики их применения, трудностей расследования, неотвратимости наказания и этических вопросов трансформирует правовые нормы в осознанные внутренние регуляторы поведения подрастающего поколения.

1.3. Правовое просвещение подростков как педагогическая задача

В свете детально проанализированной угрозы преступлений в сфере информационных технологий и ограниченной эффективности сугубо карательных мер, фокус закономерно смещается в плоскость превенции. Стратегическим ответом на вызовы цифровой эпохи становится

целенаправленное формирование правосознания у молодого поколения, для которого киберпространство является средой, в которой они проводят значительную часть своего личного и рабочего времени. Правовое просвещение подростков перерастает из факультативной воспитательной функции в ключевую педагогическую задачу национального масштаба, интегрированную в процесс обучения в школе. Ее решение – это сложный процесс воспитания внутренней культуры, этических ориентиров и поведенческих паттернов, обеспечивающих безопасность и правопорядок в цифровой среде.

Правовое просвещение представляет собой целенаправленную, систематическую деятельность по распространению правовых знаний, формированию устойчивых позитивных представлений, ценностных ориентаций и установок, обеспечивающих сознательное соблюдение, исполнение и использование юридических норм.[24] В педагогическом контексте это деятельность, ориентированная на создание условий для повышения правового сознания учащихся на основе общечеловеческих ценностей, их гражданского и профессионального становления.[25]

Отличительной чертой правового просвещения в подростковой среде является его двойственная цель. С одной стороны, это профилактическая цель: предупредить противоправное поведение, сформировав понимание недопустимости и последствий таких действий. Как показывают исследования, даже при удовлетворительном уровне формальных знаний у значительной части подростков (до 47%) наблюдается правовой нигилизм – 40% опрошенных школьников считают, что закон нужно соблюдать лишь тогда, когда он не мешает реализовывать собственные интересы.[26] Этот факт сам по себе указывает на глубокий разрыв между знанием норм и их внутренним принятием, который и призвано преодолеть правовое просвещение. С другой же стороны, это развивающая цель: воспитать активного, ответственного субъекта правовых отношений, способного

грамотно защищать свои права и свободы в цифровом пространстве, противостоять манипуляциям и кибербуллингу.

Нормативной основой для такой работы являются «Основы государственной политики Российской Федерации в сфере развития правовой грамотности и правосознания граждан», утвержденные в 2011 году.[27] Документ прямо указывает, что особое внимание должно уделяться формированию правосознания подрастающего поколения. В 2024 году Министерство просвещения Российской Федерации актуализировало этот курс, направив в регионы «Единые подходы по формированию целостной системны правового просвещения… несовершеннолетних в образовательных организациях». Эти документы задают стратегический вектор, признавая школу центральным институтом этой деятельности, поскольку именно здесь целевая аудитория принципиально доступна для целенаправленного воспитательного действия.

Однако на пути реализации этой цели стоит несколько системных проблем. Как отмечает Министерство юстиции Российской Федерации, действующее законодательство содержит пробелы: отсутствует нормативное определение правового просвещения, не закреплены его субъекты, формы, методы и критерии эффективности.[28] Это приводит к разночтениям на практике, смешение просвещения с юридической помощью или формальным информированием. Более того, существует острый кадровый дефицит: правовые знания и культура большинства взрослых, включая часть педагогов и родителей, ненамного отличаются от знаний подростков. Следовательно, эффективная работа с подростками невозможна без параллельного повышения правовой грамотности всех участников образовательного процесса – педагогов, родителей, администрации.

Эффективность педагогического воздействия напрямую зависит от учета возрастной психологии. Для подросткового возраста 14-18 лет, согласно психолого-педагогической периодизации, характерен переход к интимно-

личностному и учебно-профессиональному общению. Ведущей потребностью становится потребность в признании и самореализации, формирование «Я-концепции» в социуме. В этом возрасте подростки через призму права ищут ответы на экзистенциальные вопросы: «Какой я?», «Справедливо ли отношения других ко мне?», «Каковы границы моей свободы и ответственности?». Цифровая среда, будучи пространство для общения, самовыражения и поиска авторитетов, лишь усиливает остроту этих вопросов.

Исходя из этого, содержание правового просвещения подростков должно выходить за рамки пересказа статей Уголовного кодекса. Его ядро должно составлять формирование правовой и цифровой культуры личности, включающей:

1. Систему ценностей: приоритет человеческого достоинства, свободы, справедливости, уважения к закону и правам других – как в реальной, так и в виртуальной жизни.
2. Комплекс знаний:
    a. Основы конституционного строя и правового статуса личности.
    b. Специфика прав и обязанностей в цифровой среде – авторское право, защита персональных данных, честь и достоинство личности в сети.
    c. Уголовная и административная ответственность за ИТ-преступления – мошенничество, неправомерный доступ, кибербуллинг, распространение запрещенного контента.
    d. Механизмы защиты своих прав – обращение в правоохранительные органы, к уполномоченным по правам человека/ребенка, использование ресурсов государственных услуг.
3. Набор практических компетенций:
    a. Критическая оценка информации и ее источников.
    b. Навыки безопасного общения и поведения в социальных сетях.
    c. Умение распознавать типичные схемы кибермошенничества и манипуляций.

d. Способность конструктивно разрешать конфликты, в том числе онлайн.

Важнейшим аспектом является междисциплинарность. Правовые понятия не должны быть изолированы в рамках курса обществознания. Как показывает педагогический опыт, интересный педагогический потенциал содержит литература. Анализ правовых ситуаций в произведениях «Преступление и наказание» Ф. М. Достоевского, «Дубровский» А. С. Пушкина и в других памятниках литературы позволяет более иллюстративно обсуждать категории вины, ответственности, справедливости на эмоциональном и экзистенциальном уровне, что недостижимо при сухом разборе кодексов.[29]

Традиционный, до сих преобладающий формат – тематические уроки и лекции – критикуется специалистами как малоэффективный, особенно в контексте преподавания для подростков. Его главный недостаток – оторванность от повседневного опыта и пассивная роль ученика. Современная педагогическая практика и запрос самих подростков диктуют переход к интерактивным, деятельностным и цифроориентированным методам:

1. Имитационные и игровые методы: деловые игры, ролевые игры, правовые квесты и викторины. Они позволяют «прожить» правовую ситуацию, сформировать эмоциональный отклик и отработать модели поведения.

2. Дискуссионные формы: диспуты, дебаты, круглые столы на актуальные темы. Они развивают критическое мышление, аргументацию и умение учитывать разные точки зрения.

3. Проектная деятельность: разработка и реализация социальных проектов: создание видеороликов о кибербезопасности, мемов на правовые темы, проведение опросов среди сверстников и т. д. Это формирует активную гражданскую позицию и личную заинтересованность учеников в задании.

4. Взаимодействие с практиками: встречи с сотрудниками правоохранительных органов, работающими в сфере кибербезопасности, юристами, проведение экскурсий в суды.

Ключевой принцип – обратная связь и рефлексия. Мероприятия не должны проводиться «для галочки». Необходимо создавать условия, где подросток может задать острый, личный вопрос и получить квалифицированный, уважающий его точку зрения ответ.

Внедрение компонента по противодействию ИТ-преступлениям в систему школьного образования должно носить системный и интегрированный характер. Основной вектор – курс обществознания. Именно в его рамках, в модулях, посвященных праву, экономику и социальным отношениям, следует давать системные знания об уголовно-правовых нормах в ИТ-сфере, экономических и психологических механизмах кибермошенничества, основах защиты персональных данных. Однако, как показывают опросы, многие подростки считают только лишь предмет обществознания недостаточным для полноценного погружения, в то время как педагоги и родители чаще выступают за выделение права в отдельную дисциплину.[30] В качестве компромиссного решения мы видим проведение внеурочных тематических мероприятий, которые бы органично дополняли курс обществознания.

На наш взгляд, внеурочная деятельность и дополнительное образование предоставляют педагогам максимальную свободу творчества в вопросах выбора интерактивных форм проведения мероприятий: школьные клубы, тематические вечера, сотрудничество с волонтерами и организациями. Поле выбора достаточно широко, чтобы иметь возможность в конце концов придти к интересной для учеников форме работы.

Наконец, точно так же и необходима работа с родительским сообществом через проведение лекториев, вебинаров и рассылок, чтобы

правовые нормы и принципы кибербезопасности находили поддержку и личный пример в семье ученика.

Правовое просвещение подростков в контексте противодействия ИТ-преступлениям трансформируется из факультативной воспитательной меры в сложную, многокомпонентную педагогическую задачу, от решения которой зависит цифровая безопасность подрастающего поколения сейчас и в будущем. Ее успех возможен только при условии преодоления формализма, учета психолого-педагогических особенностей «цифрового» поколения и смещение акцента с пассивного информирования на активное, личностно-ориентированное воспитание правовой и цифровой культуры. Это требует не только разработки новых методик и интеграции в учебный процесс, но и масштабной работы по повышению квалификации педагогов и правовой грамотности родителей. Воспитание подростка, который воспринимает право не как внешнее ограничение, а как внутренний ориентир и инструмент для защиты своего достоинства в цифровом мире, становится ключевым элементом стратегической профилактики киберпреступности среди подростков.

Примичание:

[1] Сафаров, Э.А. Актуальные аспекты классификации преступлений в сфере информационных технологий: проблемы и варианты их решения // Вестник Санкт-Петербургской юридической академии. – 2024. – № 1(62). – С. 136-141.

[2] «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 20.01.2026)

[3] Белогриц-Котляревский Л.С., Сергеевский Н. Д., Фойницкий И. Я. Краткий курс русского уголовного права. М.: Ленанд. 2022. 256 с.

[4] Бавсун М.В., Векленко С.В. Квалификация преступлений по признакам субъективной стороны. М.: Юрайт. 2024. 144 с.

[5] Шевко, Н.Р. Проблемы квалификации преступлений в сфере информационных технологий // Уголовная политика в условиях трансформации : Сборник статей материалов

Всероссийской научно-практической конференции, Казань, 19 мая 2022 года. – Казань: Отечество, 2022. – С. 32-37.

[6] Понятие и виды преступлений в сфере компьютерной информации // Институт экономики и права Ивана Кушнира URL: https://be5.biz/pravo/u027/161.html (дата обращения: 27.01.2026).

[7] Уголовная ответственность и наказание / под ред. И.А. Подройкиной. М.: Юрайт. 2023. 270 с.

[8] Уголовная ответственность и наказание / под ред. А.В. Наумова, А.Г. Кибальника. М.: Юрайт. 2024. 139 с.

[9] Серебренникова, А.В. Преступления в сфере информационных технологий: кибербуллинг и кибермоббинг / А.В. Серебренникова // Проблемы экономики и юридической практики. – 2020. – Т. 16, № 2. – С. 283-287.

[10] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 09.01.2026)

[11] Сверчков В.В. Уголовное право. Общая и Особенная части. М.: Юрайт. 2023. 728 с.

[12] Ахмедханова, С.Т. Криминологическая характеристика преступлений в сфере информационных технологий / С.Т. Ахмедханова, С.Т. Ахмедханова, Э.Х. Кахбулаева // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2018. – № 4. – С. 144-152.

[13] Есаков Г.А. Российское уголовное право. Особенная часть. М.: Юрайт. 2021. 608 с.

[14] Садыкова, К.А. Некоторые проблемы раскрытия и расследования преступлений в сфере информационных технологий // Международный журнал гуманитарных и естественных наук. – 2021. – № 12-4(63). – С. 171-173.

[15] Лазарева, Л.В. Использование специальных знаний при проведении следственных действий по делам о преступлениях в сфере информационных технологий // Вестник криминалистики. – 2020. – № 2(74). – С. 87-93.

[16] Таршева, М.Н.Проблемные вопросы раскрытия и расследования преступлений в сфере информационных технологий // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 4(101). – С. 242-249.

[17] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция)

[18] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция)

[19] Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (последняя редакция)

[20] «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ (ред. от 28.12.2025)

[21] Официальный сайт Управление Генеральной прокуратуры Российской Федерации по Центральному федеральному округу» URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item=84860550 (дата обращения: 27.01.2026).

[22] Мордвинов, К.В. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. – 2022. – № 1(11). – С. 83-88.

[23] Скобликов, П.А. Стратегия борьбы с киберпреступностью: должное и сущее // Сибирское юридическое обозрение. – 2025. – Т. 22, № 1. – С. 128-146.

[24] Правовое просвещение школьников // Муниципальное бюджетное общеобразовательное учреждение города Кургана "Средняя общеобразовательная школа №44 имени Героя Советского Союза Д.М. Крутикова" URL: https://shkola12kurgan-r45.gosweb.gosuslugi.ru/roditelyam-i-uchenikam/pravovoe-prosveschenie-shkolnikov/ (дата обращения: 29.01.2026).

[25] Материалы по правовому просвещению обучающихся // МОУ "СОШ №8" URL: https://shk8-sar.gosuslugi.ru/roditelyam-i-uchenikam/materialy-po-pravovomu-prosvescheniyu-obuchayuschihsya/ (дата обращения: 29.01.2026).

[26] Решетникова, К. К. Правовое воспитание подростков: основные проблемы и пути совершенствования / К. К. Решетникова. — Текст : непосредственный // Молодой ученый. — 2021. — № 44 (386). — С. 196-198. — URL: https://moluch.ru/archive/386/84958.

[27] Единые подходы по формированию целостной системы правового просвещения и правового информирования несовершеннолетних в образовательных организациях на всех уровнях образования независимо от типа указанных организаций : приложение к письму Министерства просвещения Российской Федерации от 2 июля 2024 г. № 07-2997 // КонсультантПлюс : справочно-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_480862/.

[28] Правовое просвещение несовершеннолетних // Уполномоченный по правам ребенка в Санкт-Петербурге URL: https://www.spbdeti.org/news/pravovoe-prosveshchenie-nesovershennoletnikh/ .

[29] Правовое просвещение школьников при изучении литературы // Высшая школа делового администрирования URL: https://s-ba.ru/conf-posts-2022-04/tpost/tspfjsa8d1-pravovoe-prosveschenie-shkolnikov-pri-iz.

[30] Решетникова, К.К. Правовое воспитание подростков: основные проблемы и пути совершенствования

ГЛАВА 2. РАБОТА ПО ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИИ О ПРИМЕРАХ IT-ПРЕСТУПЛЕНИЙ В ПРОСВЕЩЕНИИ ПОДРОСТКОВ

2.1. Диагностика уровня правовой осведомленности подростков в сфере IT-преступлений

Диагностический этап нашего исследования был направлен на оценку актуального уровня правовых знаний и поведенческих установок учеников школы в отношении ИТ-преступлений. С учетом специфики цифровой среды, где подростки одновременно являются активными пользователями, и потенциальной мишенью для киберпреступников, был разработан комплексный опросник, включавший 25 вопросов. Целью диагностики было не только измерение информированности, но и выявление проблемных зон, требующих коррекции в рамках просветительской программы.

Диагностика проводилась в формате онлайн-опроса через платформу Google Forms[31] в феврале 2026. Опросник состоял из пяти тематических блоков, разработанных нами с акцентом на актуальные темы информационной безопасности:

1. Знаний понятий и видов ИТ-преступлений (вопросы на узнавание терминов: фишинг, кибербуллинг, кардинг).
2. Понимание юридических последствий и ответственности (вопросы на знание базовых положений УК РФ и возрастных границ ответственности).
3. Распознавание угроз и навыки безопасного поведения (ситуационные задачи на выбор безопасной модели поведения).
4. Оценка личных установок и поведенческих моделей (измерение самооценки уверенности и отношения к рискам по шкале).
5. Открытые вопросы для качественного анализа субъективного восприятия угроз.

Результаты опроса позволили сформировать дифференцированный портрет цифровой осведомленность школьного коллектива современной школы:

1. Высокий уровень технической грамотности при поверхностном правовом понимании – учащиеся продемонстрировали уверенное владение цифровой терминологией. Более 70% в среднем от числа всех поучаствовавших в опросе правильно определили понятия «фишинг», «кардинг», «кибербуллинг». Однако перевод этих знаний в правовое поле вызвал затруднения. Лишь 42,5% респондентов смогли правильно соотнести описанное действие, такое как «взлом Wi-Fi соседа для бесплатного использования», с соответствующим определением из Уголовного кодекса РФ. Только 47% точно знали, что уголовная ответственность за тяжкие ИТ-преступления, такие как создание вредоносных программ, наступает с 14 лет.

2. Наличие проблем понимания в соучастии и новых угроз – наиболее тревожным результатом стало отсутствие осознания рисков непреднамеренного соучастия в преступлениях. Участники с трудом понимают, где проходит тонкая грань между допустимым, но неэтичным поступком, и уголовно наказуемым деянием. Это результат согласуется с данными правоохранительных органов, отмечающих, что подростков все чаще вовлекают в схемы под «важного задания» или «работы за вознаграждения».[32] Кроме того, оказалась низкой осведомленность о новых форматах угроз – буквально пара учеников вспомнила о существовании сейчас дипфейков и ИИ-угроз, несмотря на то что сейчас это одна из самых распространенных угроз последние годы в информационном пространстве.

3. Самооценка учеников выявила следующее противоречие: абсолютное большинство оценили свою способность защитить аккаунты как высокую, но нет такого же количества уверенных, которые были бы широко осведомлены о новых угрозах, новых способах защиты и мошенничества. В открытых ответах на вопрос о самых распространенных преступлениях

преобладали бытовые формулировки, в то время как осведомленность о крупных финансовых схемах, нацеленных именно на их возрастную группу, была низкой. Между тем, статистика свидетельствует, что кибератаки на подростки 14-20 лет за последнее время резко возросли, а ущерб от мошенничеств с вовлечением детей исчисляется сотнями миллионов рублей.[33]

Проведенная диагностика подтвердила гипотезу о наличии о наличии у старшеклассников сформированной, но местами непрофильной картины цифрового восприятия мира. Учащиеся хорошо оперируют базовыми правилами «цифровой гигиена», но слабо связывают их с правовыми нормами, недооценивают риски косвенного вовлечения в преступную деятельность и не готовы действовать как полноценные субъекты правовой защиты.

Результаты четко обозначили грядущую педагогическую задачу: необходимо дать ученикам не базовые знания в очередной раз, с учетом того, что они уже хорошо владеют необходимой терминологией, а провести интерактивное мероприятие, на котором ученикам будет предоставлена возможность поучаствовать в разрешении правовых конфликтов на основе реальных ситуаций из российского информационного пространства. Практически ориентированный интенсив, на наш взгляд, в большей степени сможет поспособствовать формированию знаний и навыков ориентирования в современном пространстве, насыщенном различными информационными угрозами. Следовательно, для разработки программы просветительских мероприятий был выбран игровой формат анализа конкретных кейсов (англ. «case-study»).[34] Этот метод позволит нам в рамах данного мероприятия:

1. Работать со свежими, актуальными инфоповодами, такими как «Дело Долиной».[35] что резко повышает интерес и вовлеченность аудитории.
2. Моделировать сложные, этически неоднозначные ситуации, где нет единственно правильно ответа, что стимулирует критическое мышление и навыки дискуссии.

3. На практике отрабатывать алгоритмы действий – от распознавания угрозы до грамотного описания деяния для правоохранительных органов.

4. Наглядно демонстрировать, как теоретические положения УК РФ применяются к реальным жизненным обстоятельствам, тем самым углубляя правопонимания.

Проведенная диагностика не только констатировала текущий уровень осведомленности, но и, выявив его качественные характеристики, стала основанием для проектирования подходящей, закрывающей проблемные ниши, формы просветительской деятельности.

2.2. Разработка и реализация программы просветительских мероприятий для подростков

Результаты первичной диагностики, выявившие противоречие между формальной информированностью подростков и недостаточной глубиной их правопонимания, предопределили ключевой вектор проектирования просветительской программы. Для нашего исследовательского состава стало очевидно, что традиционные лекционные форматы для просветительских мероприятий не способный эффективно сформировать у старшеклассников устойчивые навыки правовой оценки сложных цифровых ситуаций.

В качестве методического ядра был избран интерактивный формат case-study (анализа конкретных ситуаций), который позволяет перенести фокус с пассивного усвоения информации на активное обсуждение и дискуссию о правовых и морально-этических аспектах. Разработанное внеурочное мероприятие «Анализ реальных кейсов ИТ-преступлений и выработка правовой позиции» представляет собой педагогическую модель, направленную на преодоление выявленных ранее дефицитов: преодоление

правового нигилизма, осознание рисков непреднамеренного соучастия и формирования алгоритма поведения для избегания небезопасных для подростков ситуаций.

Выбор формата работы в малых группах, названных «Юридическими бюро», является нашим дидактическим решением, отвечающим возрастным особенностям старшеклассников, для которых ведущей деятельностью является личностное и учебно-профессиональное общение. Групповая работа создает безопасную среду для высказывания гипотез, обоснование своих собственных мнений и совместного поиска решения, что, на наш взгляд, принципиально важно для усвоения сложных этико-правовых категорий. Формат кейса, в свою очередь, моделирует реальную профессиональную деятельность – от анализа первичных фактов до формирования своей позиции и ее защиты в ходе обсуждения. Такой подход позволяет реализовывать принцип деятельностного обучения, переводя знания из категории «знаю, что» в категорию «знаю и анализирую, применяю, аргументирую». Хронометраж мероприятия в 90 минут позволяет в достаточной степени проработать практическую составляющую данного мероприятия.

Представленные для анализа пять кейсов, который мы старались тщательно подбирать на основании критериев актуальности для современных школьников и удовлетворения их образовательных запросов, образуют содержательное ядро мероприятия. Они фокусируются на наиболее уязвимых для подростков сферах жизни в сети. Кейсы №1 «Звонок из деканата» и №4 «Фишинг на Avito» посвящены классическим схемам мошенничества с использованием социальной инженерии, где ключевой задачей для учащихся становится идентификация «красных флагов» – манипулятивных приемов и признаков обмана. Вопросы в этих кейсах нацелены на развитие превентивного мышления: «На каком этапе нужно было прервать диалог?», «Какие правила безопасной сделки были нарушены?». Особую дидактическую силу кейсам придает использование резонансных инфоповодов, таких как

«Дело Долиной» в качестве аналога, что позволяет масштабировать частную ситуацию со студентом до уровня громкого судебного процесса, демонстрируя универсальность механизмов мошенничества и выступая как понятный и узнаваемый пример.

Другой вариант проблематизации представляют кейсы, посвященные рискам превращения из жертвы в соучастника. Кейс №2 «Дроппер и деньги» является центральным с точки зрения профилактики непреднамеренного криминализации подростков. Опираясь на шокирующую статистику роста дропперства в 74 раза с 2020 по 2025 года, работа с этим кейсом заставляет учащихся отвечать на вопрос: «Почему эта схема преступна, даже если сам подросток ничего не воровал?». Изучение статьи УК РФ в контексте реальной истории 17-летнего подростка позволяет материализовать абстрактную правовую модель в реальную связь «легкой подработки» в Telegram и уголовным правом.

Кейсы №3 «Шутка о минировании» и №5 «Месть в сети» выводят обсуждение на тему ответственности за действия в сети и защиту человеческого достоинства в виртуальной среде. К сожалению, до сих пор часто проскальзывают новости о намеренных, часто шуточных, несерьезных сообщениях от минирования, которые в том числе крайне часто исходят из школьников, которые могут и не понимать опасность самого явления терроризма, ровно, как и не осознают масштабы уголовной ответственности за подобного рода «шутку», поэтому разбор подобных кейсов мы считаем крайне актуальным и уместным. Точно также явление кибербуллинга только набирает обороты в сети и, к сожалению, пока нет оснований говорить о снижении частоты проявления данного явления в сети среди подростков. Конфликтность, обоснованная психолого-возрастными особенностями подростков, часто становится основанием для такого рода «травли». Несмотря на то, что сильнее всего страдает жертва травли, от кибербуллинга страдает и сам «буллер», он же задира и хулиган, зачинщик конфликта. Поэтому

приведение и разбор такого кейса нацелен на обращение внимание учеников на неубывающую актуальность травли в сети среди подростков. Такие кейсы способствуют развитию эмпатии, показывая, что от подобного страдает моральный коллектив всего коллектива. Это позволяет говорить о формировании не только правовой, но и гражданской культуры среди учеников.

Преимущество за методом кейсов при выборе подхода мы увидели в возможности дать ученикам не просто ситуацию на анализ, а ее отражение в нескольких источниках, описывающих одно правовое явление под разными углами: с точки зрения новостных заголовков, статьи Уголовного кодекса Российской Федерации и аналогичных ситуаций из реальной жизни. Такой подход позволяет отвечать на вызовы современности – высокие требования к навыкам критического мышления людей, которые мы отрабатываем через работу с документами и групповую дискуссию. В конце мероприятия предполагается финальная дискуссия по всем кейсам, сопровождающаяся «последним словом» ведущего для подведения итогов работы. Ученики вряд ли узнают что-то новое из такого материала – но это и не нужно. По работе с детьми, особенно подростками-старшеклассниками можно понять, что они и так с этим всем были знакомы. Цель мероприятия в другом – придать этому знакомому «смысл». Все эти ситуации ученики достаточно часто наблюдают как в собственной жизни, так и в медиапространстве вокруг себя, но обычно они не предают этому такого значения. Поэтому данное мероприятие и должно проводиться именно для того, чтобы ученики поняли, что это не «рядовое событие» или «легкая подработка», а что каждый раз они находятся на пересечении тонкой грани, отделяющей их действия от уголовно наказуемого деяния.

Значимым, но часто упускаемым из виду аспектом подобной методики является ее мощный воспитательный потенциал, направленный на формирование правосознания. Правосознание здесь понимается не как сума

знаний, а как комплекс установок, включающих уважение к закону, чувство личной ответственности и внутреннюю готовность действовать правомерно даже в условиях анонимности виртуальной среды. Работа в группах над этически и морально сложными кейсами провоцирует ценностно-смысловую рефлексию со стороны учеников. Учащиеся так или иначе приходят к вопросам об их роли в конфликтных ситуациях, мошеннических схемам и реакции на подобные события в социуме. Такой внутренний диалог способствует оформлению правовых норм во внутренние регуляторы личности учеников, подобно нормам морали.

Содержание нашего плана мероприятия основано на актуальных и социально значимых событиях из жизни учеников, что позволяет обеспечить высокий уровень заинтересованности и внутренней мотивации к решению поставленных задач. Подобный интенсив позволяет ученикам в игровой и познавательной форме работы развить навыки критического мышления, аргументированной дискуссии, саморефлексии через анализ ситуаций, в которых им удалось побывать за свою жизнь. При разработке данного мероприятия, помимо восполнения познавательных дефицитов учеников, нашей главной целью, все-таки, было преодоление вечной проблемы многих просветительских мероприятий – лекционный характер через донесение до учеников фактов, о которых они и так уже знают. Мы же старались не сказать им повторно об этих фактах, а наполнить эту информацию смыслом, придать ей более важное значение в их понимании, чтобы в дальнейшем на подобные ситуации ученики уже смотрели с большим вниманием.

2.3. Анализ эффективности проведенной работы и методические рекомендации для преподавателей

Апробация разработанного просветительского мероприятия «Анализ реальных кейсов ИТ-преступлений и выработка правовой позиции» была осуществлена на базе 11-х классов МАОУ Гимназии №15 города Красноярска. Мероприятие проводилось в рамках внеурочной деятельности и было направлено на проверку педагогической гипотезы о том, что интерактивный, проблемно-ориентированный формат способен преодолеть выявленный на этапе диагностики разрыв между фактическими знаниями и пониманием работы права на практике.

Организационно мероприятие было проведено в соответствии с разработанным конспектом, однако живой учебный процесс внес коррективы в хронометраж. Основная сложность, появившаяся на этапе работу в группах, заключалась в неравномерной вовлеченности учащихся. В нескольких группах инициативу взяли на себя 1-2 уверенных ученика, в то время как остальные ограничились пассивным слушанием и высказыванием поверхностных позиций. Решить эту классическую проблему в процессе мероприятия удалось за счет точечного вовлечения учеников в дискуссию самим педагогом через дополнительные вопросы и просьбы высказать свое мнение более развернуто. Вторая, более значимая, трудность была связана с работой над нормативными источниками. Несмотря на предоставленные выдержки из Уголовного кодекса РФ, часть групп испытывала значительные трудности с интерпретацией юридических формулировок, таких как «приобретение права на чужое имущество путем модификации компьютерной информации» (ст. 159.6). Учащиеся, как правило, стремились давать морально-бытовую оценку, но с трудом переводили ее в правовое поле, что замедляло анализ. Временные рамки работы над всеми кейсами в совокупности были превышены примерно на 10-12 минут, преимущественно

за счет этапа групповой работы, что указывает на необходимость более тщательной проработки в дальнейшем.

Несмотря на отмеченные ранее трудности, наблюдение за работой групп и финальной дискуссией позволили зафиксировать ряд положительных сдвигов, свидетельствующих о достижении ключевой цели – формировании основ правовой оценки ситуаций и иного взгляда на привычные действия. Наиболее заметным результатом стало изменение качества аргументации к моменту обсуждения последнего кейса. Если в начале мероприятия преобладали уже обозначенные нами ранее морально-бытовые оценки, то к концу обсуждения последнего кейса ученики уже тщательнее обращали внимание на юридически состав преступления по текстам статьи и активно подключали данные факты к своей аргументации.

Особую ценность такого мероприятия составила выработка превентивных моделей поведения. При обсуждении кейса «Фишинг на Avito» группы, помимо обозначения «красных флагов» в диалоге, смогли сформировать вполне очевидные и точные правила совершения подобных операций в сети, чтобы избежать случаев мошенничества. Не столь очевидным результатом мы находим повышение уровня правовой рефлексии. Мы дали ученикам возможность более внимательно взглянуть на достаточно распространенные случаи, чтобы они могли обратить внимание на то, что такие ситуации носят куда более деструктивный характер для общественных отношений, чем они раньше полагали. Мы склонны считать, что ученики, учитывая их сегодняшнюю возможность к самообучению, уже были знакомы с большей частью идей мероприятия, однако данные кейсы смогли подтолкнуть их переосмыслению и иначе взглянуть на рядовые ситуации, чтобы осознать их потенциальные риски и общественную опасность для всех окружающих.

По результатам проведения мы можем сформировать несколько рекомендаций для педагогов, которые в будущем по нашим конспектам захотят повторить проведение подобного мероприятия.

В случае необходимости, помимо текста кейса и статей УК РФ, рекомендуется разработать для учащихся краткий глоссарий ключевых юридических терминов. Это снимает терминологический барьер и ускорит погружение в суть задания. В нашем опыте это оказалось необходимо сильно меньше, но тенденция на уместность разработки подобного материала прослеживалась отчетливо.

Для предотвращения пассивности участников, особенно, если они будут из более младших параллелей, целесообразным будет заранее определить или предложить группам выбрать внутри себя роли для участников: модератора для отслеживания работы команды, аналитика для выписывания важнейших фактов кейса, главного спикера для защиты результатов работы группы и других. Это поможет формализовать учебный процесс и гарантирует участие каждого.

Учитель должен быть готов активно перемещаться между группами, задавая «тонкие» вопросы, которые бы помогали направлять мысли учеников в правильное русло мышления: «Какое конкретно действие здесь незаконно?», «Можно ли в данном случае говорить о соучастии?». Так можно создать более благоприятную атмосферу для проведения самостоятельного анализа учениками.

Следует закладывать резерв времени 5-7 минут на преодоление неизбежных задержек. Финальную дискуссию необходимо завершать не формальным выводом, а еще раз рефлексивно кругом пройтись по всем заданиям и собрать конечные итоги воедино, чтобы не упустить важных мыслей, которые могли остаться где-то в середине активной работы. Это поможет в закреплении личностного смысла деятельности, если дать ученикам

самостоятельно высказать итоговые тезисы на основе проведенной на мероприятии работы.

В теории, для усиления эффекта и закрепления усвоенного опыта, целесообразно было бы предложить ученикам развитие данного мероприятия в научно-исследовательскую деятельность с подготовкой статей о, к примеру, подростковой преступности или актуальной степени уязвимости подростков в интернете. Так получится не только реализовывать проектные и исследовательские возможности активных учеников, но и перевести их новые знания в иную плоскость применения.

Практическая апробация данного внеурочного мероприятия, как мы считаем, указала на достаточно высокий образовательный и воспитательный потенциал разработанной методики. Несмотря на возникшие организационные и содержательные препятствия и трудности, которые носят закономерный и преодолимый характер, мероприятие достигло своей главной цели – оно инициировало процесс пересмотра и анализа знакомых для учеников ситуаций в ином, более правовом ключе, чтобы в дальнейшем способствовать проявлению превентивной модели поведения у учеников. В ходе самого процесса работы это тоже частично прослеживалось. Ученикам удавалось замечать, что ситуации, о которых они нередко слышали в новостях или от знакомых, на самом деле носили куда более серьезные последствия для подростков и всего социума, чем они до этого предполагали. Такое рефлексивное переосмысление указывает на реализацию оригинальной задумки. Учащиеся не только познакомились с конкретными статьями Уголовного кодекса, но и поработали над механизмом их интерпретации, навыками критического мышления и сформировали основу для ответственного поведения в цифровой информационной среде. Программа указала на эффективность подобного подхода в качестве модели правового просвещения, который можно рекомендовать к внедрению в практику работы в современных образовательных учреждениях для решения актуальной задачи

профилактики ИТ-преступности в подростковой и молодежной среде как в роли инициаторов, так и случайных жертв.

Примичание:

[1]Google Forms // Google [Электронный ресурс] URL: https://docs.google.com/forms (дата обращения: 10.02.2026).

[2] Возрастные разграничения: мошенники в 1,5 раза чаще стали атаковать детей // Известия [Электронный ресурс] URL: https://iz.ru/1925249/valerii-kodachigov/vozrastnye-razgranicheniya-moshenniki-v-1-5-raza-chashche-stali-atakovat-detej (дата обращения: 10.02.2026).

[3] Опасные игры: в 2025 г. мошенники похитили через атаки на детей более 850 млн рублей // Safe News [Электронный ресурс] URL: https://safe.cnews.ru/news/line/2025-11-17_opasnye_igry_v_2025_gmoshenniki (дата обращения: 10.02.2026).

[4] Бодога, Е. А. Образовательный потенциал использования кейс-метода на уроках истории / Е. А. Бодога // Актуальные вопросы гуманитарных наук : Сборник научных статей бакалавров, магистрантов и аспирантов. – Москва : ИКД "Зерцало-М", 2024. – С. 20-25.

[5] Эффект Долиной: как одно уникальное дело запустило череду судебных ошибок и что делать с добросовестным приобретателем теперь // zakon.ru [Электронный ресурс] URL: https://zakon.ru/blog/2025/10/8/effekt_dolinoj_kak_odno_unikalnoe_delo_zapustilo_cheredu_sudebnyh_oshibok_i_chto_delat_s_dobrosovest (дата обращения: 10.02.2026).

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило осуществить всесторонний анализ феномена ИТ-преступности в контексте подростковой среды и разработать эффективную методику осуществления правового просвещения и профилактики подростковой преступности в сети. Теоретический анализ позволяет утверждать, что преступления в сфере информационных технологий представляют собой сложную, динамическую систему деяний, где цифровые средства выступают как инструментом, так и средой совершения противоправных действий. Установлено, что эволюция киберпреступности характеризуется не только технологическим усложнением, но и активным вовлечением молодежи, которая в силу возрастных психологических особенностей и высокой цифровой вовлеченности оказывается в группе риска как в роли жертвы, так и в роли невольного или осознанного соучастника. Систематизация видов и способов таких преступлений показывает возможность представления и визуализации этих материалов для мероприятий по правому просвещению школьников.

Уголовно-правовая характеристика российского законодательства в исследуемой области показала, что действующая система норм, сосредоточенная в главе 28 УК РФ и ряде смежных составов, образует комплексный, хотя и постоянно требующий актуализации, механизм противодействия. Однако анализ статистики и оценок выявил ключевое противоречие: при всей жесткости санкций и развитости правовых конструкций, репрессивные меры не могут в одиночку решить проблему, поскольку ее корни лежит в сфере правосознания и цифровой культуры населения.

Нами было показано, что эффективное просвещение подростков должно выходить за рамки разового информирования о статьях закона. Его стратегической целью является формирование целостной цифровой правовой

культуры, интегрирующей устойчивые ценностные ориентации, системные знания и практические навыки безопасного и ответственного поведения в виртуальном пространстве.

Несмотря на хорошее владение базовой цифровой грамотностью, учащиеся продемонстрировали серьезные проблемы в понимании юридических последствий своих действий, неумении квалифицировать свои действия в рамках уголовного законодательства и незнании механизмов правовой защиты. Особенно тревожным оказался низкий уровень осознания рисков непреднамеренного соучастия в таких схемам, как дропперство. Эти результаты наглядно показали неэффективность традиционных форм информирования и просветительской деятельности.

В ответ на выявленные дефициты была разработана и подробно описана программа просветительского мероприятия, основанная на методе анализа конкретных ситуации – метод кейсов. Его методическим ядром стала работа в группах над смоделированными, но основанными на реальных и актуальных инфоповодах кейсами, охватывающими спектр основных угроз: от социальной инженерии и мошенничества до кибербуллинга и ложных сообщений об опасности. Программа была структурирована таким образом, чтобы учащиеся самостоятельно, через изучение первоисточников и коллективную дискуссию, выявляли правовую суть ситуации, учились применять нормативные акты и формировать алгоритмы безопасного поведения.

Практическая апробация данной программы в условиях реального учебного процесса и ее последующий анализ доказали общую состоятельность и показательную эффективность избранного формата. Несмотря на возникшие организационные сложности, такие как неравномерная активность в группах и первоначальные трудности с интерпретацией юридических текстов, мероприятие достигло своих ключевых целей. Качественный анализ работы учащихся показал переход от бытовых оценок к сознательному

использованию правовых понятий, а главное – формирование осознания личной ответственности и конкретных механизмов защиты в цифровой среде. На основе рефлексии этого опыта были сформулированы конкретные методические рекомендации для педагогов.

Проведенное исследование в полной мере достигло своей основной цели, заключавшейся в определении наиболее эффективных форм работы со школьниками в рамках правового просвещения об угрозах ИТ-преступности и кибербезопасности. Эффективность правового просвещения подростков в данной сфере напрямую зависит от его практической ориентированности, интерактивности и связи с актуальным жизненным контекстом обучающихся. Программа на основе кейс-метода показала свою способность преодолевать формализм в знаниях, формируя у старшеклассников целостное правосознание, критическое мышление и устойчивые навыки правомерного поведения в цифровом пространстве. Результаты исследования могут быть непосредственно внедрены в систему внеурочной деятельности, внося существенный вклад в решение одной из наиболее острых проблем современного общества – обеспечения правовой безопасности молодого поколения в условиях цифровой трансформации.

СПИСОК ЛИТЕРАТУРЫ И ИСТОЧНИКОВ

Источники

Нормативно-правовые акты

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 09.01.2026)

2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 28.12.2025)

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025) (с изм. и доп., вступ. в силу с 20.01.2026)

4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

6. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ

Интернет-ресурсы

7. Google Forms // Google URL: https://docs.google.com/forms (дата обращения: 10.02.2026).

8. Ваша цифровая и правовая грамотность // Google URL: https://forms.gle/UaxvBoEudy1J5cHY7 (дата обращения: 09.02.2026).

9. Возрастные разграничения: мошенники в 1,5 раза чаще стали атаковать детей // Известия URL: https://iz.ru/1925249/valerii-kodachigov/vozrastnye-razgranicheniya-moshenniki-v-1-5-raza-chashche-stali-atakovat-detej (дата обращения: 10.02.2026).

10. Единые подходы по формированию целостной системы правового просвещения и правового информирования несовершеннолетних в образовательных организациях на всех уровнях образования независимо от

типа указанных организаций : приложение к письму Министерства просвещения Российской Федерации от 2 июля 2024 г. № 07-2997 // КонсультантПлюс : справочно-правовая система. —URL: https://www.consultant.ru/document/cons_doc_LAW_480862/ (дата обращения: 29.01.2026).

11. Материалы по правовому просвещению обучающихся // МОУ "СОШ №8" URL: https://shk8-sar.gosuslugi.ru/roditelyam-i-uchenikam/materialy-po-pravovomu-prosvescheniyu-obuchayuschihsya/ (дата обращения: 29.01.2026).

12. Опасные игры: в 2025 г. мошенники похитили через атаки на детей более 850 млн рублей // Safe News URL: https://safe.cnews.ru/news/line/2025-11-17_opasnye_igry_v_2025_gmoshenniki (дата обращения: 10.02.2026).

13. Официальный сайт Управление Генеральной прокуратуры Российской Федерации по Центральному федеральному округу». URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item=84860550 (дата обращения: 27.01.2026).

14. Понятие и виды преступлений в сфере компьютерной информации // Институт экономики и права Ивана Кушнира [Электронный ресурс] URL: https://be5.biz/pravo/u027/161.html (дата обращения: 27.01.2026).

15. Правовое просвещение несовершеннолетних // Уполномоченный по правам ребенка в Санкт-Петербурге URL: https://www.spbdeti.org/news/pravovoe-prosveshchenie-nesovershennoletnikh/ (дата обращения: 29.01.2026).

16. Правовое просвещение школьников // Муниципальное бюджетное общеобразовательное учреждение города Кургана "Средняя общеобразовательная школа №44 имени Героя Советского Союза Д.М. Крутикова" URL: https://shkola12kurgan-r45.gosweb.gosuslugi.ru/roditelyam-i-uchenikam/pravovoe-prosveschenie-shkolnikov/ (дата обращения: 29.01.2026).

17. Правовое просвещение школьников при изучении литературы // Высшая школа делового администрирования URL: https://s-ba.ru/conf-posts-

2022-04/tpost/tspfjsa8d1-pravovoe-prosveschenie-shkolnikov-pri-iz (дата обращения: 29.01.2026).

18. Решетникова, К. К. Правовое воспитание подростков: основные проблемы и пути совершенствования / К. К. Решетникова. — Текст : непосредственный // Молодой ученый. — 2021. — № 44 (386). — С. 196-198. — URL: https://moluch.ru/archive/386/84958

19. Эффект Долиной: как одно уникальное дело запустило череду судебных ошибок и что делать с добросовестным приобретателем теперь // zakon.ru URL: https://zakon.ru/blog/2025/10/8/effekt_dolinoj_kak_odno_unikalnoe_delo_zapustilo_cheredu_sudebnyh_oshibok_i_chto_delat_s_dobrosovest (дата обращения: 10.02.2026).

Литература

20. Ахмедханова, С. Т. Криминологическая характеристика преступлений в сфере информационных технологий // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2018. – № 4.

21. Бавсун М. В., Векленко С. В. Квалификация преступлений по признакам субъективной стороны. М.: Юрайт. 2024.

22. Белогриц-Котляревский Л. С., Сергеевский Н. Д., Фойницкий И. Я. Краткий курс русского уголовного права. М.: Ленанд. 2022.

23. Бодога, Е. А. Образовательный потенциал использования кейс-метода на уроках истории // Актуальные вопросы гуманитарных наук : Сборник научных статей бакалавров, магистрантов и аспирантов. – Москва : ИКД "Зерцало-М", 2024.

24. Есаков Г. А. Российское уголовное право. Особенная часть. М.: Юрайт. 2021.

25. Лазарева, Л. В. Использование специальных знаний при проведении следственных действий по делам о преступлениях в сфере информационных технологий // Вестник криминалистики. – 2020. – № 2(74).

26. Мордвинов, К. В. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью // Теоретическая и прикладная юриспруденция. – 2022. – № 1(11).

27. Садыкова, К. А. Некоторые проблемы раскрытия и расследования преступлений в сфере информационных технологий // Международный журнал гуманитарных и естественных наук. – 2021. – № 12-4(63).

28. Сафаров, Э. А. Актуальные аспекты классификации преступлений в сфере информационных технологий: проблемы и варианты их решения // Вестник Санкт-Петербургской юридической академии. – 2024. – № 1(62).

29. Сверчков В. В. Уголовное право. Общая и Особенная части. М.: Юрайт. 2023.

30. Серебренникова, А. В. Преступления в сфере информационных технологий: кибербуллинг и кибермоббинг // Проблемы экономики и юридической практики. – 2020. – Т. 16, № 2.

31. Скобликов, П. А. Стратегия борьбы с киберпреступностью: должное и сущее // Сибирское юридическое обозрение. – 2025. – Т. 22, № 1.

32. Таршева, М. Н. Проблемные вопросы раскрытия и расследования преступлений в сфере информационных технологий // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2024. – № 4(101).

33. Уголовная ответственность и наказание / под ред. А. В. Наумова, А. Г. Кибальника. М.: Юрайт. 2024.

34. Уголовная ответственность и наказание / под ред. И. А. Подройкиной. М.: Юрайт. 2023.

35. Шевко, Н. Р. Проблемы квалификации преступлений в сфере информационных технологий // Уголовная политика в условиях трансформации : Сборник статей материалов Всероссийской научно-

практической конференции, Казань, 19 мая 2022 года. – Казань: Отечество, 2022.

ПРИЛОЖЕНИЯ

Приложение 1.

Электронная версия:

Ваша цифровая и правовая грамотность // Google URL: https://forms.gle/UaxvBoEudy1J5cHY7 (дата обращения: 09.02.2026).

Опросник «Ваша цифровая и правовая грамотность»

Уточнение: ваши результаты тестирования будут *анонимизированными* и представлены *как общая статистика*

Вопрос №0. Поделитесь с нами, из какого вы класса?

- 5 класс
- 6 класс
- 7 класс
- 8 класс
- 9 класс
- 10 класс
- 11 класс

Блок А. Знание основных понятий и видов ИТ-преступлений.

1. Что такое «фишинг»?
    a. Вид интернет-рекламы
    b. Рассылка сообщений с целью выманивания конфиденциальной информации
    c. Кража персональных данных из утерянного человеком телефона
2. Кибербуллинг – это…
    a. Взлом аккаунтов в социальных сетях

b. Травля, оскорбления, угрозы, распространение слухов в цифровом пространстве
c. Покупка товаров в интернете с украденной карты

3. Какое из перечисленных действий НЕ является ИТ-преступлением согласно Уголовному кодексу РФ?
   a. Публикация в соцсети чужой фотографии без согласия, когда это не привело к негативным последствиям для личности
   b. Создание провокационного мема на основе кадра из фильма
   c. Взлом школьного электронного журнала для изменения оценок
4. «Кардинг» – это преступление, связанное с…
   a. Незаконным копированием и распространением компьютерного софта
   b. Мошенничество с использованием чужих реквизитов банковских карт
   c. Долговременное продолжающееся преследование человека в сети
5. Что означает аббревиатура «DDos-атака»?
   a. Вирус, шифрующийся на данном компьютере
   b. Массовая рассылка спам-писем
   c. Намеренный вывод из строя сайта или сервера путем огромного количества запросов

Блок Б. Понимание юридических последствий и ответственности

6. С какого возраста в РФ наступает уголовная ответственность за тяжкие преступления в сфере ИТ?
   a. С 14 лет
   b. С 16 лет
   c. С 18 лет
7. Если подросток «угадал» пароль к Wi-Fi соседа, чтобы пользоваться им бесплатно, это может быть квалифицировано как…

a. Ничего страшного, если не возникло негативных последствий для жизни соседа
b. Неправомерный доступ к компьютерной информации
c. Мелкое хулиганство

8. Распространение в мессенджере фейковой новости о минировании школы «в шутку» может повлечь…
   a. Только дисциплинарное наказание для ученика
   b. Административную или уголовную ответственность за заведомо ложное сообщение об акте терроризма
   c. Блокировку аккаунта в этой социальной сети
9. Продажа в интернете скачанной из нелицензионного источника музыки или фильма под видом собственного товара – это…
   a. Нарушение авторских прав и мошенничество
   b. Ненаказуемая предпринимательская деятельность
   c. Нарушение, за которое не предусмотрена серьезная ответственность
10. Максимальное наказание по статье УК РФ за создание и распространение вредоносных программ, повлекшее тяжкие последствия, может достигать…
    a. Штрафа до 10 тыс. руб.
    b. Лишения свободы на срок до 10 лет
    c. 160 часов обязательных общественных работ

Блок В. Распознавание угроз и навыки безопасного поведения

11. Какой из предложенных паролей является наиболее надежным?
    a. «123!45a7»
    b. «qwerty&*1»
    c. «J7@kL92#mN1!»
12. Вам пришло сообщение «Ваша карта заблокирована. Срочной перейдите по ссылке bank-help.ru для разблокировки. Что делаете?

a. Последую инструкции
b. Свяжусь со своим банком в приложении или по телефонному номеру, чтобы проверить информацию
c. Проигнорирую

13. В соцсети вам пишет незнакомец, представляясь сверстником из школы, просит ваши данные от Электронного дневника, чтобы сверить домашнее задание. Что дальше?
    a. Отправить, если человек вызывает доверие
    b. Вежливо отказать и прекратить общение
    c. Послать данные других людей, если есть
14. Вы нашли в сети взломанный премиум-аккаунт популярного стримингового сервиса. Можно ли им пользоваться?
    a. Да, я что, каждый день такую удачу ловлю, чтобы ее упускать?!
    b. Нет, это использование неправомерного доступа к информации
    c. Можно, если использовать режим «Инкогнито»
15. Двухфакторная аунтефикация нужна для…
    a. Ускорения входа в аккаунт с вашего нового устройства
    b. Повышения уровня защиты даже в случае утечки пароля
    c. Рассылки рекламы

Блок Г. Оценка личных установок и моделей поведения

Оцените свое согласие со следующими утверждениями по шкале от 1 («Полностью НЕ согласен») до 5 («Полностью согласен»).

16. Я уверен, что знаю, как защитить свои аккаунты в соцсетях от взлома
    a. 1, 2, 3, 4, 5
17. Мне известно, куда и как можно обратиться, если я стал жертвой мошенничества или травли в интернете
    a. 1, 2, 3, 4, 5
18. Я считаю, что ответственность за ИТ-преступления для несовершеннолетних незначительная и им всегда «прощают»

a. 1, 2, 3, 4, 5

19. При скачивании фильмов, музыки или игр с пиратских сайтов я задумываюсь о возможных юридических последствиях
    a. 1, 2, 3, 4, 5
20. Я считаю, что угрозы или оскорбления в сети – это не серьезно, особенно в сравнении с «реальной» жизнью»
    a. 1, 2, 3, 4, 5

Блок Д. Источники знаний и самооценка грамотности

21. Откуда вы в основном получаете информацию о безопасном поведении в интернете и правовом поле? (Можно выбрать несколько)
    a. Школьные уроки
    b. Родители
    c. Соцсети, блогеры
    d. Новости в СМИ
    e. Собственный опыт/опыт друзей
22. Как вы оцениваете в целом свой уровень правовых знаний в Digital-сфере?
    a. Высокий
    b. Средний
    c. Низкий
23. Как вы думаете, насколько актуально для ваших сверстников проблема вовлечения в ИТ-преступления (как жертв или нарушителей)?
    a. Очень актуальна
    b. Довольно актуальна
    c. Не очень актуальна
    d. Совсем не актуальна

Блок Е. Открытые вопросы

24. Как вы думаете, какое ИТ-преступление самое распространенное среди подростков и почему?

_____

_____

_____

_____

25. Какая, на ваш взгляд, самая эффективная мера, чтобы уберечь подростков от нарушений закона в сети? Дайте краткое объяснение выбора

_____

_____

_____

_____

Приложение 2.

Ключи для обработки и интерпретации информации.

- Блоки А, Б, В (вопросы 1-15): оценивается по бинарной школе – правильно или неправильно. Сумма правильных ответов позволяет говорить о степени сформированности объективного индекса правовых знаний (ИПЗ).
- Блок Г (вопросы 16-20): оценивается по баллам. Для позитивных утверждений – 16,17, 19 – баллы суммируются как есть, то есть ответ «5» = 5 баллов. Для негативных утверждений – 18, 20 – баллы инвертируются, то есть ответ «5» = 1 баллу и т. д. Итог – индекс субъективной уверенности и адекватности установок (ИСУ).
- Блок Д (Вопросы 21-23): анализируется частотным методом по проценту выбравших каждый вариант ответа.
- Блок Е (Вопросы 24-25) анализируется качественно по содержанию.

Данный опросник и его методика оценивания позволят получить данные об объективном уровне знаний, субъективных оценках и поведенческих предрасположенностях учеников.

Электронная версия:

Ваша цифровая и правовая грамотность // Google [Электронный ресурс] URL: https://forms.gle/UaxvBoEudy1J5cHY7 (дата обращения: 09.02.2026).

Приложение 3.

План-конспект внеурочного мероприятия.

Тема «Анализ реальных кейсов ИТ-преступлений и выработка правовой позиции»

Цель: формирование у учеников критического мышления, навыков правовой оценки ситуации в цифровой среде и осознание личной ответственности.

Актуальность: количество ИТ-преступлений, совершенных среди несовершеннолетних, с 2020 по 2024 год выросло в 74 раза. Каждое пятое преступление подростка совершается в интернете. Молодежь все чаще становится не только жертвами, но и соучастниками, часто даже не осознавая последствий.

Формат: учитель организует группы «юридические бюро» по 4-5 человек с последующей презентацией и обсуждением их решений. В каждое бюро одновременно отсылается кейс по ИТ-преступлению, на основе реальных случаев. После его изучения и обдумывания идет дискуссия с участием всех бюро и педагогов для подведения итогов ситуации и вынесения оценки действиям.

Хронометраж до 90 минут:

- Введение (10 мин)
- Работа над кейсами (до 70 мин)
- Подведение итогов и финальная дискуссия (10 мин)

Содержание кейсов:

№	Название кейса	Суть ситуации	Источники для анализа	Вопросы для группы
1	«Звонок из деканата»	Студенту звонит «сотрудник деканата», сообщает о проблеме с	1. Статья РБК о признаках влияния мошенников	1. Дайте общую оценку ситуации

		документами и просит для их проверки продиктовать код из СМС от Госуслуг. После этого аккаунт студента используется для получения кредита	2. Текст УК РФ, ст. 159.6 3. Аналог кейса из реальной жизни	2. На каком этапе нужно было прервать диалог? 3. Какие меры защиты своего аккаунта вы знаете? 4. Какова роль человеческого фактора в данной ситуации?
2	«Дроппер и деньги»	Школьнику в Телеграмме предлагают «легкую подработку»: открыть на свое имя банковскую карту или получить посылку и перевести деньги, оставив себе процент. Он соглашается, считая это безопасным	1. Статья о росте «дропперства» среди подростков 2. Текст УК РФ, статья 174.1 3. Аналог кейса из реальной жизни	1. Дайте общую оценку ситуации 2. Почему эта схема преступна, даже если сам подросток ничего не воровал? 3. Какой ущерба наносится общественным отношениям? 4. Как бы вы аргументировали отказ, если бы предложение поступило другу или от него?
3	«Шутка о минировании»	Ученик, поссорившись с учителем, анонимно пишет в чат класса: «Завтра в школу лучше не приходить, будет жарко». Сообщение быстро расходится по соцсетям, вызывая панику у всех	1. Статья, где ложные сообщения об опасности названы частым подростковым явлением 2. Текст УК РФ, ст. 207 3. Аналог кейса из реальной жизни	1. Дайте общую оценку ситуации 2. С какого момента шутка становится преступлением? 3. Каков расчет морального и материального ущерба от такой шутки? 4. Как следует поступить, если такую ситуацию увидел ты? 5. Как бы ты поступил, если бы узнал, что твой друг расстроен и собирается сделать подобное?

4	«Фишинг на Avito»	Покупатель на Avito хочет купить у школьника PlayStation по выгодной цене. Просит перейти по ссылке для гарантии сделки от Avito ввести данные карты для возврата залога. Деньги с карты исчезают	1. Статья о мошенничестве на торговых площадках 2. Текст УК РФ ст. 159.6 3. Аналог кейса из реальной жизни	1. Дайте общую оценку ситуации 2. Какие «красные флаги» могут быть в такой переписке? 3. Какие правила безопасной сделки на площадках были нарушены? 4. Какие первые действия, когда вы понимаете, что стали жертвой такой ситуации?
5	«Месть в сети»	После конфликта одноклассники создают фейковую страницу ученика выкладывают его «отфотошопленные» селфи и личные переписки. Жертва получает травлю и угрозы здоровью, что приводит к тяжелому стрессу	1. Статья ООН о масштабах кибербуллинга 2. Текст УК РФ, ст. 128.1, ст. 119 3. Аналог кейса из реальной жизни	1. Дайте общую оценку ситуации 2. Какова разница между обычным конфликтом и преступлением в цифровой среде? 3. Какие права человека были нарушены? 4. Алгоритм действий жертвы: куда и с какими доказательствами обращаться? 5. Хорошо подумайте, кому от такой ситуации становится плохо и кому нужна помощь?

Приложение 4.

КЕЙС №1. «ЗВОНОК ИЗ ДЕКАНАТА»

Суть ситуации: Студенту звонит «сотрудник деканата», сообщает о проблеме с документами и просит для их проверки продиктовать код из СМС от Госуслуг. После этого аккаунт студента используется для получения кредита.

Вопросы:

1. Дайте общую оценку ситуации

2. На каком этапе нужно было прервать диалог?

3. Какие меры защиты своего аккаунта вы знаете?

4. Какова роль человеческого фактора в данной ситуации?

Материалы для изучения:

Статья «В МВД перечисли признаки влияния мошенников на подростка»

Появление у детей новых дорогих вещей и техники, наличие чужих банковских карт и определенная лексика могут указывать на то, что ребенок оказался под влиянием мошенников, сообщает ТАСС со ссылкой на данные МВД России. К явным признакам влияния мошенников на подростка относятся частое и скрытное проведение времени в интернете, появление денег неизвестного происхождения и специфическая лексика: «дропы», «кладмены», «спортики», «клад», «закладка», «симка», «ворк», «аренда акка». Кроме того, маркером могут служить специфические предметы: изолента, маленькие зип-пакеты, магниты, множество сим-карт, чужие банковские карты и реквизиты. По данным ведомства, за первые семь месяцев 2025 года почти 5 тыс. детей и подростков стали жертвами преступлений, совершенных

с использованием информационно-телекоммуникационных технологий, что на 25% больше, чем годом ранее. В ведомстве добавили, что в России потерпевшими от противоправных посягательств чаще всего являются люди в возрасте от 25 до 44 лет. Для этого злоумышленники используют секретные чаты, анонимные группы с обсуждением «заработка», закрытые каналы с такими вакансиями, как дропы, кладмены, симки, админы. По данным специалистов, среди способов вовлечения подростков также выделяются боты-вербовщики. Речь идет об автоматизированных сервисах, которые рассылают предложения «о работе» или создают чаты знакомств, предлагая подросткам быстрый и легкий заработок.

УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

(в ред. Федерального закона от 03.07.2016 N 325-ФЗ)

(см. текст в предыдущей редакции)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) лицом с использованием своего служебного положения;

б) в крупном размере;

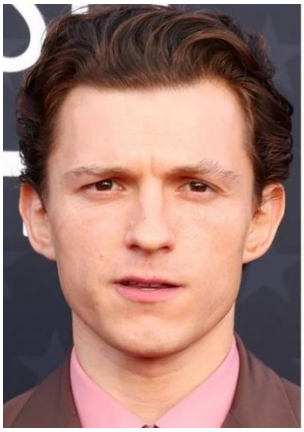
в) с банковского счета, а равно в отношении электронных денежных средств, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

«Дело Долиной»



Летом 2024 года певица Лариса Долина стала жертвой телефонных мошенников, убедивших её продать квартиру в Хамовниках (за 112 млн руб.) и перевести деньги на «безопасные

счета». Поняв обман, певица пыталась оспорить сделку. В конце 2025 года Верховный суд РФ окончательно признал право собственности за покупательницей Полиной Лурье, отказав в возврате квартиры. Основные факты дела: аферисты представлялись сотрудниками ФСБ, убедив артистку, что ее квартира находится в опасности, и что продажа — это часть «спецоперации». Ущерб: певица потеряла квартиру и перевела более 200 млн руб. (с учетом продажи) курьерам.

Судебные тяжбы: изначально суды (Хамовнический, Мосгорсуд) признавали сделку недействительной. Однако Верховный суд в декабре 2025 года отменил эти решения, признав покупателя Полину Лурье добросовестной стороной.

Последствия: квартира осталась у покупателя, а Долиной предстоит взыскивать средства с мошенников. Дело вызвало огромный резонанс,

повысив риски при покупке «вторички» и запустив дискуссию о защите прав покупателей. В настоящее время ведется уголовное дело, часть курьеров задержана.

Приложение 5.

КЕЙС №2. «ДРОППЕР И ДЕНЬГИ»

Суть ситуации: школьнику в Телеграмме предлагают «легкую подработку»: открыть на свое имя банковскую карту или получить посылку и перевести деньги, оставив себе процент. Он соглашается, считая это безопасным.

Вопросы:

1. Дайте общую оценку ситуации

2. Почему эта схема преступна, даже если сам подросток ничего не воровал?

3. Какой ущерба наносится общественным отношениям?

4. Как бы вы аргументировали отказ, если бы предложение поступило другу или от него?

Материалы для изучения:

Статья «За 4 года количество ИТ-преступлений, совершенных детьми, выросло в 74 раза. Злоумышленники все чаще втягивают подростков в дропперство».

Число ИТ-преступлений, совершенных детьми и подростками, выросло с 2020 года в 74 раза. Об этом сообщил старший инспектор по особым поручениям Главного управления по обеспечению охраны общественного порядка субъектов МВД России Артем Бабинцев.

«За последние 4 года, по данным официальной нашей статистики МВД, в 74 раза возросло количество ИТ-преступлений, совершенных именно лицами, не достигшими 18 лет. То есть, если в 2020 году это количество было 54 преступления, то в 2023 году мы зафиксировали уже 4 тыс. таких

преступлений. Это свидетельствует о том, что технологии развиваются, вовлечение в цифровую криминальную среду подростков тоже развивается. Это вызывает у нас определенное беспокойство», — рассказал он на Форуме безопасного интернета, который прошел в Москве.

Количество преступлений с использованием ИТ в целом выросло на 30% только за последний год, а ущерб от них превысил 156 млрд рублей, напомнил член комитета Госдумы по информационной политике, информационным технологиям и связи Антон Немкин. По его словам, за 12 лет Роскомнадзор заблокировал порядка 130 тысяч материалов, направленных на вовлечение несовершеннолетних в опасные деяния. Особенно активно распространяются материалы, вовлекающие в опасную и противозаконную деятельность, на зарубежных платформах – например, в социальной сети Likee. Кроме того, в криминальных схемах все чаще оказываются замешаны подростки, которые открывают на свое имя банковские счета, получают карты и передают их третьим лицам либо самостоятельно снимают со счетов похищенные деньги, чтобы передать их преступникам.

По его словам, сегодня важно найти эффективный способ борьбы с таким явлением как дропперство — использованием мошенниками граждан, которые соглашаются предоставлять свои счета и документы для вывода украденных средств, подчеркнул Немкин. «На сегодняшний более 60% дропперов — младше 24 лет, а многие становятся ими уже с 14 лет — когда получают возможность открыть в банке счет и завести карту. Таким образом злоумышленники вовлекают в противоправную деятельность подростков, которые зачастую даже не осознают, на что подписываются. При этом нужно понимать — это не просто этическая проблема, это преступление, за которое придется ответить. Наша задача — оградить молодежь от таких опасных шагов, которые могут в дальнейшем сильно повлиять на их будущее», — заключил парламентарий.

УК РФ Статья 174.1. Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления

1. Совершение финансовых операций и других сделок с денежными средствами или иным имуществом, приобретенными лицом в результате совершения им преступления, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года.

2. То же деяние, совершенное в крупном размере, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на срок до двух лет со штрафом в размере до пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев либо без такового.

3. Деяния, предусмотренные частью первой или второй настоящей статьи, совершенные:

а) группой лиц по предварительному сговору;

б) лицом с использованием своего служебного положения, -

наказываются принудительными работами на срок до трех лет с ограничением свободы на срок до двух лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до пяти лет со штрафом в размере до пятисот тысяч рублей или в

размере заработной платы или иного дохода осужденного за период до трех лет или без такового, с ограничением свободы на срок до двух лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

4. Деяния, предусмотренные частью первой или третьей настоящей статьи, совершенные:

а) организованной группой;

б) в особо крупном размере, -

наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет или без такового, с ограничением свободы на срок до двух лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Статья «17-летний подросток из Нижегородской области сознался полиции в дропперстве»

17-летний подросток из Уреня сознался полицейским в дропперстве. Об этом сообщили в пресс-службе ГУ МВД России по Нижегородской области.

Молодой человек нашел в Сети подработку и связался с «работодателем». По указанию аферист он представил свои данные, а затем стал получать на свой счет денежные средства. В последующем несовершеннолетний отправлял суммы на сторонние реквизиты. За свою

«работу» он получил 2400 рублей. Из-за большого числа переводов карта подростка была заблокирована, а общение с «нанимателем» прекратилось.

Школьник сообщил в полицию о своем преступлении и написал явку с повинной.

Возбуждено уголовное дело по факту неправомерного оборота средств платежей. Фигуранту выдали подписку о невыезде и надлежащем поведении.

Приложение 6.

КЕЙС №3. «ШУТКА О МИНИРОВАНИИ»

Суть ситуации: ученик, поссорившись с учителем, анонимно пишет в чат класса: «Завтра в школу лучше не приходить, будет жарко». Сообщение быстро расходится по соцсетям, вызывая панику у всех.

Вопросы:

1. Дайте общую оценку ситуации

2. С какого момента шутка становится преступлением?

3. Каков расчет морального и материального ущерба от такой шутки?

4. Как следует поступить, если такую ситуацию увидел ты?

5. Как бы ты поступил, если бы узнал, что твой друг расстроен и собирается сделать подобное?

Материалы для изучения:

Статья «Почти 20% совершенных подростками преступлений произошли в Интернете или с использованием компьютеров»

«Почти 20% всех преступлений, совершенных подростками, произошли в Сети или с использованием компьютерных технологий. Детская преступность перетекает с улицы в Интернет», — отметил Роман Бардеев.

Родители должны знать, чем занимается их ребенок в Интернете. При этом не должно быть тотального контроля, так как несовершеннолетний может замкнуться в себе и пытаться избегать такого надзора. «В данном случае хорошим подспорьем для обеспечения безопасности ребенка могут стать программы родительского контроля. Данные приложения ограничивают те или иные функции гаджета. Таким образом можно отгородить ребенка от

неблагоприятных сайтов, длительного пребывания в Интернете или играх, а также не допустить его ознакомления с нежелательным контентом», — подчеркнул старший инспектор.

Он также отметил, что 50% мошенничеств совершается в виртуальном пространстве. Как правило, такие преступления происходят на торговых онлайн-площадках или в соцсетях, где публикуются объявления о продаже товаров по заниженным ценам. Обязательным условием в таком случае становится внесение предоплаты или задатка. Зачастую после перечисления денег покупатель остается ни с чем, а продавец перестает выходить на связь и удаляет свои аккаунты.

Самое распространенное киберпреступление, совершаемое подростками, — хищение имущества путем модификации компьютерной информации. Как правило, подростки создают фишинговую ссылку, с помощью которой получают сведения о реквизитах банковской карты человека. После этого при помощи специальных программ несовершеннолетние похищают с карты деньги. Одними из самых часто совершаемых подростками преступлений в Сети являются заведомо ложное сообщение об опасности и вымогательство.

В летний период возрастает вероятность вовлечения детей в совершение противоправных деяний. Поэтому максимальные усилия сотрудников ОВД совместно с Министерством образования в этот период направлены на организацию занятости детей, повышение уровня их цифровой грамотности и проведение различных профилактических мероприятий в оздоровительных и пришкольных лагерях. Кроме того, МВД во взаимодействии с заинтересованными органами на постоянной основе принимает превентивные меры по предупреждению киберпреступлений. Проводятся разъяснительные беседы в учреждениях образования, трудовых коллективах, в СМИ и интернете размещается тематическая информация. Дважды в год проводятся масштабные республиканские профилактические акции, одна из которых была

реализована перед каникулами. Также правоохранители организуют творческие конкурсы, интерактивные акции и другие мероприятия по тематике кибербезопасности.

«Кроме профилактической работы МВД также принимает меры по блокировке сайтов и аккаунтов с неприемлемым контентом. Организовано круглосуточное взаимодействие с Национальным банком Республики Беларусь по обработке информации о несанкционированных платежных операциях, что позволяет оперативно принимать решения об их приостановлении. На законодательном уровне реализуются инициативы, направленные на урегулирование сделок с криптовалютой, квалификацию деяний, связанных с незаконным оборотом средств платежа», — отметил Роман Бардеев.

УК РФ Статья 207. Заведомо ложное сообщение об акте терроризма

1. Заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, совершенное из хулиганских побуждений, -

наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо принудительными работами на срок от двух до трех лет.

2. Деяние, предусмотренное частью первой настоящей статьи, совершенное в отношении объектов социальной инфраструктуры либо повлекшее причинение крупного ущерба, -

наказывается штрафом в размере от пятисот тысяч до семисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет либо лишением свободы на срок от трех до пяти лет.

3. Заведомо ложное сообщение о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий в целях дестабилизации деятельности органов власти, -

наказывается штрафом в размере от семисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок от шести до восьми лет.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, повлекшие по неосторожности смерть человека или иные тяжкие последствия, -

наказываются штрафом в размере от одного миллиона пятисот тысяч до двух миллионов рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет либо лишением свободы на срок от восьми до десяти лет.

Примечания. 1. Крупным ущербом в настоящей статье признается ущерб, сумма которого превышает один миллион рублей.

2. Под объектами социальной инфраструктуры в настоящей статье понимаются организации систем здравоохранения, образования, дошкольного воспитания, предприятия и организации, связанные с отдыхом и досугом, сферы услуг, пассажирского транспорта, спортивно-оздоровительные учреждения, система учреждений, оказывающих услуги правового и финансово-кредитного характера, а также иные объекты социальной инфраструктуры.

Статья «Двух подростков из Тюмени и Челябинска будут судить за ложное минирование в Брянске»

Двое несовершеннолетних из хулиганских побуждений решили совершить ложное сообщение о минировании одного из крупных административных зданий в Советском районе Брянска.

Молодые "минеры" заранее нашли в интернете сведения о брянце для звонка от его имени. Использовали компьютерную программу для звонков через интернет.

Накануне Дня города, вечером 16 сентября 2025 года, подростки позвонили с номера из диапазона иностранных государств в дежурную часть УМВД России по Брянской области, соврав о минировании административного здания в центре.

Следователем проведен большой объем следственных действий в Брянской, Тюменской и Челябинской областях. Были добыты доказательства причастности обвиняемых, расследование завершено, уголовное дело направлено в суд.

Приложение 7.

КЕЙС №4. «ФИШИНГ НА AVITO»

Суть ситуации: покупатель на Avito хочет купить у школьника PlayStation по выгодной цене. Просит перейти по ссылке для гарантии сделки от Avito ввести данные карты для возврата залога. Деньги с карты исчезают.

Вопросы:

1. Дайте общую оценку ситуации

2. Какие «красные флаги» могут быть в такой переписке?

3. Какие правила безопасной сделки на площадках были нарушены?

4. Какие первые действия, когда вы понимаете, что стали жертвой такой ситуации?

Материалы для изучения:

Статья «Почти 20% совершенных подростками преступлений произошли в Интернете или с использованием компьютеров»

«Почти 20% всех преступлений, совершенных подростками, произошли в Сети или с использованием компьютерных технологий. Детская преступность перетекает с улицы в Интернет», — отметил Роман Бардеев.

Родители должны знать, чем занимается их ребенок в Интернете. При этом не должно быть тотального контроля, так как несовершеннолетний может замкнуться в себе и пытаться избегать такого надзора. «В данном случае хорошим подспорьем для обеспечения безопасности ребенка могут стать программы родительского контроля. Данные приложения ограничивают те или иные функции гаджета. Таким образом можно отгородить ребенка от неблагоприятных сайтов, длительного пребывания в Интернете или играх, а

также не допустить его ознакомления с нежелательным контентом», — подчеркнул старший инспектор.

Он также отметил, что 50% мошенничеств совершается в виртуальном пространстве. Как правило, такие преступления происходят на торговых онлайн-площадках или в соцсетях, где публикуются объявления о продаже товаров по заниженным ценам. Обязательным условием в таком случае становится внесение предоплаты или задатка. Зачастую после перечисления денег покупатель остается ни с чем, а продавец перестает выходить на связь и удаляет свои аккаунты.

Самое распространенное киберпреступление, совершаемое подростками, — хищение имущества путем модификации компьютерной информации. Как правило, подростки создают фишинговую ссылку, с помощью которой получают сведения о реквизитах банковской карты человека. После этого при помощи специальных программ несовершеннолетние похищают с карты деньги. Одними из самых часто совершаемых подростками преступлений в Сети являются заведомо ложное сообщение об опасности и вымогательство.

В летний период возрастает вероятность вовлечения детей в совершение противоправных деяний. Поэтому максимальные усилия сотрудников ОВД совместно с Министерством образования в этот период направлены на организацию занятости детей, повышение уровня их цифровой грамотности и проведение различных профилактических мероприятий в оздоровительных и пришкольных лагерях. Кроме того, МВД во взаимодействии с заинтересованными органами на постоянной основе принимает превентивные меры по предупреждению киберпреступлений. Проводятся разъяснительные беседы в учреждениях образования, трудовых коллективах, в СМИ и интернете размещается тематическая информация. Дважды в год проводятся масштабные республиканские профилактические акции, одна из которых была реализована перед каникулами. Также правоохранители организуют

творческие конкурсы, интерактивные акции и другие мероприятия по тематике кибербезопасности.

«Кроме профилактической работы МВД также принимает меры по блокировке сайтов и аккаунтов с неприемлемым контентом. Организовано круглосуточное взаимодействие с Национальным банком Республики Беларусь по обработке информации о несанкционированных платежных операциях, что позволяет оперативно принимать решения об их приостановлении. На законодательном уровне реализуются инициативы, направленные на урегулирование сделок с криптовалютой, квалификацию деяний, связанных с незаконным оборотом средств платежа», — отметил Роман Бардеев.

УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные:

а) лицом с использованием своего служебного положения;

б) в крупном размере;

в) с банковского счета, а равно в отношении электронных денежных средств, -

наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, -

наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного

дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Статья «Многодетные супруги из Красноярa потеряли 50 000 рублей, покупая стройматериалы на «Авито»

Итак, супруги искали подешевле ОСБ-плиту для обшивки дома. В магазинах она стоит сейчас порядка 830 рублей за лист. На «Авито» нашли несколько объявлений с ценой меньше, но в разговоре с продавцом каждый раз выяснялось, что цена уже выросла. И только третье объявление — ОСБ по 589 рублей/лист — оказалось актуальным.

— Продавец, представившийся Дмитрием, объяснил, что они продают только оптовые партии, поэтому такая цена, — рассказывает Наталья. — Опт — от одного поддона, поддон — 78 штук, нам на дом чуть поменьше надо, но на баню пригодится.

Кстати, дешевизна — одна из приманок у мошенников, и, если предлагают что-то ценное нереально дешево (под предлогом, например, срочности) — почти наверняка где-то кроется подвох. В данном случае цена, в общем-то, не была совсем уж низкой, чтобы это могло насторожить. Ну а отсутствие отзывов у продавца (показатель надежности) вполне объяснялось «свежестью» регистрации — 17 июня 2024 года. Ведь все когда-то с чего-то начинают. «Документы проверены, телефон подтвержден», опять же.

Дальше Дмитрий заработал еще несколько очков в свою пользу, сообщив в переписке в чате на сервисе, что предоплату не нужно, оплата — после доставки, по факту, на карту.

— Но нет возможности самовывоза — только собственная доставка, — продолжает Наталья. — Стоимость доставки в Красноярск — 3300 рублей, тоже, в общем-то, нормально. Итого 49 242 рубля. Экономия выходила

существенная — почти 16 тысяч, как если бы покупать в том же «Леруа». Конечно, мы согласились, заняли денег.

Дальнейшее общение с продавцом происходило в вотсапе по номеру, указанному Дмитрием. Покупатели написали адрес, объяснили, как ехать. Договорились на завтра — субботу, 22 июня.

— Утром звонит: машина выехала, ожидайте. Единственное, попросил, чтобы мы не разговаривали о цене товара с водителем: мол, с сегодняшнего дня цену подняли, но раз мы с вами вчера договорились… Прибыла «газель», два молодых парня. На машине реклама какой-то компании. Парни начали выгружать товар на полянку. Я пошла платить. Дмитрий скинул в вотсап реквизиты, банк отклонил операцию, с сообщением, что данному клиенту платеж невозможен, превышен лимит, повторите попытку через 24 часа. Я отправила скриншот Дмитрию. Он прислал другой счет, потом еще один. Перевести удалось только на третий и частями. В течение часа мы этим занимались. Обменялись смайликами на прощание.

Все это время водитель и грузчик спокойно сидели на полянке рядом с привезенными плитами. Когда Наталья сказала им, что перевела деньги, водитель позвонил своему начальству, выяснилось, что денег не поступало: если в течение 15 минут оплаты не будет, загружайте все обратно и уезжайте, приказали ему. А из мессенджера, как обнаружила Наталья, исчезли все сообщения Дмитрия, и абонент сразу стал «не абонент».

— И только после этого они предъявили нам бумажную накладную. Заказчиком в ней значился Дмитрий и был указан его телефон (то есть тот номер, по которому велись все переговоры). И сумма там была указана другая — 62 720 рублей (78 листов ОСБ по 740 рублей за штуку и 5000 рублей доставка).

То есть Дмитрий заказал ОСБ-плиту с оплатой по факту на адрес Натальи и Алексея. Просто и гениально.

Покупателям пришлось вернуть выгруженные поддоны с плитами. 50 000 рублей ушли аферисту. Его объявление снято с публикации.

— Если бы мы сразу увидели накладную, конечно, обман бы вскрылся, — сетует Наталья. — Но нам и в голову это не пришло. Мы ведь все увидели, потрогали, вот оно все лежит, уже наше, какие тут могут быть сомнения? Очень технично нас провели, не подкопаешься. Все предусмотрели. К примеру, я бы решила рассчитаться наличкой с водителем — но ведь нас Дмитрий предупредил, что он не в курсе стоимости. Понятно, что ты не захочешь подводить человека, оказывающего тебе услугу.

Супруги написали заявление в полицию. Они очень надеются, что мошенника поймают и заставят возместить ущерб, 50000 рублей — большая сумма для семьи с четырьмя детьми (трое — маленькие), которая, к тому же, строится. А рассказать об их печальном опыте в СМИ потерпевшие решили, чтобы предупредить земляков, что такое бывает.

Не исключено, что этот Дмитрий (или Марина, или Петр) уже снова выставил свое заманчивое — ровно настолько, чтобы при этом выглядеть реальным — объявление.

Молодые люди, доставившие товар в Красноярск, дали Наталье рекламный буклет своей компании — «Урал-Плит» из Среднеуральска (тот же логотип был и на автомобиле). Мы позвонили в «Урал-Плит» по указанному в буклете телефону. Ответивший мужчина сказал, что они в курсе истории. Компания потеряла и свои деньги — на доставке груза (бензин, зарплата водителю и грузчику). По словам менеджера, действительно, заказ был сделан по телефону, оплата у них всегда по факту. «Такого у нас не бывало. Мы тоже приняли меры во избежание подобных обманов. Теперь при заказе пробиваем номер по специальной программе, и, если он «засвечен» в каких-то подозрительных операциях или вообще не бьется, просим предоплату», — добавил менеджер.

Ну а доставщиков желательно бы обязать в первую очередь предъявлять клиенту накладную, чтобы он мог удостовериться, что ему привезли именно то, что он заказал, и по той цене. А также реквизиты для оплаты.

Приложение 8.

КЕЙС №5. «МЕСТЬ В СЕТИ»

Суть ситуации: после конфликта одноклассники создают фейковую страницу ученика выкладывают его «отфотошопленные» селфи и личные переписки. Жертва получает травлю и угрозы здоровью, что приводит к тяжелому стрессу.

Вопросы:

1. Дайте общую оценку ситуации

2. Какова разница между обычным конфликтом и преступлением в цифровой среде?

3. Какие права человека были нарушены?

4. Алгоритм действий жертвы: куда и с какими доказательствами обращаться?

5. Хорошо подумайте, кому от такой ситуации становится плохо и кому нужна помощь?

Материалы для изучения:

Статья ООН «Безопасность детей и молодежи в Интернете»

Молодые люди в возрасте от 15 до 24 лет чаще пользуются Интернетом, чем остальное население, однако за последние четыре года этот разрыв между поколениями постепенно сокращается. Согласно пересмотренным оценкам, в 2023 году Интернетом будут пользоваться около 77 процентов людей в возрасте от 15 до 24 лет. Но вместе с этими возможностями приходят и серьезные риски. Кибербуллинг и другие формы насилия со стороны сверстников могут затрагивать молодых людей каждый раз, когда они заходят в социальные сети или на платформы обмена мгновенными сообщениями.

Более трети молодых людей в 30 странах сообщают, что подвергались кибербуллингу, а каждый пятый прогуливал школу из-за этого.

При работе в Интернете дети и подростки могут столкнуться с разжиганием ненависти и насилием, включая сообщения, подстрекающие к членовредительству и даже самоубийству. Молодые пользователи Интернета также уязвимы для вербовки экстремистскими и террористическими группами.

Цифровые платформы также используются для распространения дезинформации и теорий заговора, которые оказывают вредное воздействие на детей и подростков.

Наибольшую тревогу вызывает угроза сексуальной эксплуатации и насилия в Интернете. Никогда еще не было так легко для детей, совершивших сексуальные преступления, связаться со своими потенциальными жертвами, поделиться изображениями и побудить других к совершению преступлений. Около 80% детей в 25 странах сообщают, что чувствуют себя в опасности сексуального насилия или эксплуатации в Интернете.

Дети также могут подвергаться риску, когда технологические компании нарушают их конфиденциальность для сбора данных в маркетинговых целях. Маркетинг, ориентированный на детей, через приложения - и чрезмерное время, проведенное за экраном, - может поставить под угрозу здоровое развитие ребенка.

Безграничный характер Интернета означает, что обеспечение безопасности молодых людей в сети является глобальной задачей. ООН активно работает над защитой детей и молодежи в Интернете с помощью различных программ и инициатив.

Инициатива по защите детей в Интернете (COP) — это многосторонняя сеть, созданная Международным союзом электросвязи (МСЭ) с целью повышения осведомленности о безопасности детей в Интернете и разработки

практических инструментов для оказания помощи правительствам, промышленным предприятиям и педагогам. Руководство МСЭ по защите детей в Интернете представляет собой всеобъемлющий набор рекомендаций для всех соответствующих заинтересованных сторон о том, как внести свой вклад в развитие безопасной и расширяющей возможности детей и молодежи среды в Интернете.

Детский фонд ООН (ЮНИСЕФ) объединился с платформами социальных сетей, чтобы ответить на некоторые из наиболее распространенных вопросов о киберзапугивании и дать советы о том, как с ним бороться. Эта инициатива ЮНИСЕФ направлена на то, чтобы положить конец киберзапугиванию.

Каждый первый четверг ноября Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО) отмечает Международный день борьбы с насилием и запугиванием в школе, включая киберзапугивание, признавая, что насилие в школе во всех его формах является нарушением прав детей и подростков на образование, здоровье и благополучие. Этот день дает возможность заинтересованным сторонам во всем мире активизировать усилия по обеспечению безопасности учащихся в школе и в онлайн-пространстве.

ЮНИСЕФ предотвращает сексуальную эксплуатацию детей в Интернете и реагирует на нее на страновом и глобальном уровнях. Он поддерживает скоординированные национальные меры по борьбе с сексуальной эксплуатацией детей в Интернете в более чем 20 странах, используя модель глобального альянса WePROTECT, укрепляя потенциал специалистов на местах по оказанию услуг жертвам.

Всемирная организация здравоохранения (ВОЗ) в своем отчете за 2022 год о предотвращении онлайн-насилия в отношении детей уделяет особое внимание сексуальному насилию над детьми, включая груминг и

надругательство над сексуальным образом, а также кибер-агрессию и домогательства. В докладе подчеркивается важность реализации образовательных программ, ориентированных на детей и родителей.

Торговля людьми — это преступление, в результате которого люди становятся объектом торговли и эксплуатации в корыстных целях. Торговцы людьми стали умело использовать интернет-платформы для вербовки жертв и привлечения клиентов. Дети и подростки подвержены обманным уловкам в поисках признания, внимания или дружбы, и часто «обхаживаются» торговцами людьми в социальных сетях. Управление ООН по наркотикам и преступности (УНП ООН) поддерживает государства-члены в их усилиях по предотвращению и борьбе с торговлей людьми, в том числе посредством мероприятий по повышению осведомленности о безопасности в Интернете, направленных на детей и подростков.

ЮНЕСКО возглавляет глобальные усилия по разработке нормативных решений для повышения достоверности информации на цифровых платформах в условиях роста дезинформации. В феврале 2023 года агентство ООН провело конференцию «Интернет, как источник достоверной информации», на которой обсуждался ряд глобальных руководящих принципов, направленных на создание безопасной и надежной интернет-среды для пользователей при защите свободы выражения мнений и доступа к информации. Руководство призывает цифровые платформы признать свою особую ответственность перед детьми. Поскольку в детском возрасте происходит становление личности. При этом возможности детей влиять на принятие мер директивного характера крайне ограничены.

ЮНЕСКО также является ведущим учреждением ООН по продвижению медийной и информационной грамотности (МИГ), которая дает людям возможность критически осмысливать информацию и использовать цифровые инструменты. ЮНЕСКО стремится вооружить молодежь навыками медийной и информационной грамотности, чтобы они могли стать активными

участниками процесса создания и распространения знаний и информации о ресурсах МИГ. С 2016 года ЮНЕСКО проводит Форум молодежной повестки дня, чтобы помочь молодым людям узнать о последних достижениях в области МИГ. Это часть ежегодной Глобальной недели медийной и информационной грамотности — важной возможности для заинтересованных сторон проанализировать и отметить прогресс, достигнутый на пути к медийной и информационной грамотности для всех.

Права детей закреплены в Конвенции о правах ребенка. Комитет ООН по правам ребенка (КПР), который следит за выполнением Конвенции, определил, как следует обращаться с молодыми людьми и детьми в цифровом мире и как следует защищать их права.

Комитет провел консультации с правительствами, гражданским обществом и более чем 700 детьми и подростками в 27 странах, спрашивая их, как цифровые технологии влияют на их права и какие действия они хотели бы видеть предпринятыми для их защиты. Выводы были изложены в «Замечании общего порядка».

Комитет рекомендовал государствам принять решительные меры, в том числе законодательного характера, для защиты детей от вредного и вводящего в заблуждение контента. Дети также должны быть защищены от всех форм насилия, происходящего в цифровой среде, включая торговлю детьми, гендерное насилие, кибер-агрессию, кибер-атаки и информационную войну.

Взгляды и опыт детей необходимо учитывать при разработке директивных мер, регулирующих использование молодежью цифровых технологий, а также при разработке самих технологий. ЮНИСЕФ поддерживает проекты Global Kids Online и Disrupting Harm, направленные на сбор данных о цифровых правах, возможностях и рисках для детей, чтобы лучше понять, как использование цифровых технологий способствует их развитию и когда оно усиливает риск причинения им вреда.

Учреждения ООН и партнеры, включая новаторов из частного сектора, работают над повышением безопасности в Интернете, особенно для детей и молодежи. При поддержке МСЭ, ЮНИСЕФ и ЮНОДК День безопасного Интернета отмечается ежегодно в феврале месяце. День безопасного Интернета направлен на повышение осведомленности о новых проблемах и вызовах в цифровой сфере.

УК РФ Статья 128.1. Клевета

1. Клевета, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо обязательными работами на срок до ста шестидесяти часов.

2. Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть "Интернет", либо в отношении нескольких лиц, в том числе индивидуально не определенных, -

наказывается штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до двухсот сорока часов, либо принудительными работами на срок до двух лет, либо арестом на срок до двух месяцев, либо лишением свободы на срок до двух лет.

3. Клевета, совершенная с использованием своего служебного положения, -

наказывается штрафом в размере до двух миллионов рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до трехсот двадцати часов, либо принудительными работами на срок до трех лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до трех лет.

4. Клевета о том, что лицо страдает заболеванием, представляющим опасность для окружающих, -

наказывается штрафом в размере до трех миллионов рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо обязательными работами на срок до четырехсот часов, либо принудительными работами на срок до четырех лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до четырех лет.

5. Клевета, соединенная с обвинением лица в совершении преступления против половой неприкосновенности и половой свободы личности либо тяжкого или особо тяжкого преступления, -

наказывается штрафом в размере до пяти миллионов рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо принудительными работами на срок до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до пяти лет.

УК РФ Статья 119. Угроза убийством или причинением тяжкого вреда здоровью

1. Угроза убийством или причинением тяжкого вреда здоровью, если имелись основания опасаться осуществления этой угрозы, -

наказывается обязательными работами на срок до четырехсот восьмидесяти часов, либо ограничением свободы на срок до двух лет, либо

принудительными работами на срок до двух лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное:

а) по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы;

б) в отношении лица или его близких в связи с осуществлением данным лицом служебной деятельности или выполнением общественного долга;

в) с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть "Интернет"), -

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Статья «Школьники из Татарстана пожаловались Мизулиной на буллинг»

Школьники из Татарстана направили обращения главе «Лиги безопасного интернета» Екатерине Мизулиной, рассказав о случаях буллинга в учебных заведениях. В письмах дети описывают ситуации травли, связанной с особенностями внешности и личностными характеристиками.

Одна из учениц, проживающая в неназванном городе республики, поделилась историей о том, как ее и одноклассницу подвергают насмешкам из-за лишнего веса. Девочка отметила, что заступается за подругу, которая, по ее словам, из-за веса испытывает сложности с поиском друзей: окружающие позволяют себе грубые высказывания в ее адрес.

Другая школьница из Казани рассказала, что сталкивалась с буллингом во всех трех учебных заведениях, где ей довелось учиться.

— Учителя вообще не делают ничего, просто говорят, что это мои проблемы и дело в том, что болтлива и много агрессирую. Ну а как мне еще реагировать на такое, я просто не пойму, — поделилась девочка.

Екатерина Мизулина сообщила, что получает значительное количество писем, посвященных проблеме травли в школах.

— В предложке шквал писем по поводу травли в школах. Каждое второе письмо на эту тему. Пишут как те, кто уже пережил эту ситуацию, так и ребята, которые сталкиваются с этим прямо сейчас. Многие говорят о том, что в школах эти проблемы игнорируют или вообще обвиняют во всем тех, кто этой травле и подвергается, — отметила она.

В августе депутаты ЛДПР предложили ввести штрафы до 500 тыс. рублей за буллинг и кибербуллинг. За лицо, не достигшее 16 лет, ответственность будут нести родители или опекуны. Штрафы за буллинг для физлиц могли составить от 10 тыс. до 50 тыс., для юрлиц — от 100 тыс. до 500 тыс., для должностных лиц — от 100 тыс. до 200 тыс. рублей.

Позднее, в сентябре, депутаты «Новых людей» предложили министру цифрового развития Максуту Шадаеву внедрить дополнительные механизмы защиты детей от буллинга в онлайн-сообществах. Соответствующее письмо направлено министру.