**Материал для ИПГ, 18 ноября, 2021 г. Чериков**

**МЕДИАКУЛЬТУРА И МЕДИАПОТРЕБЛЕНИЕ В БЕЛОРУССКОМ ОБЩЕСТВЕ**

В условиях глобальной информатизации общества и возрастающей скорости протекания всех социальных процессов, основная роль в формировании ценностных ориентаций личности и общества, сохранении исторической памяти переходит к медиакультуре, средствам массовой информации (далее – СМИ).

Сегодня в информационном пространстве наиболее активно развиваются новые медиа –мультимедийные многоканальные персонализированные интернет-ресурсы. Интернет давно стал одним из основныхисточников получения новостей и пространством для общения.

На совещании с руководителями ведущих государственных СМИ 11 февраля 2020 г.Глава государства А.Г.Лукашенко подчеркнул: *«Сегодня Интернет уже не просто дышит в спину государственной прессе, но и по некоторым позициям вырывается вперед, а Telegram-каналы, блоги, социальные сети по влиянию как минимум сравнялись с традиционными СМИ. Молодежь в основном там.*

*Мобильный телефон с выходом в Интернет в распоряжении всех желающих: от ребенка до пожилого человека. И эти материалы им доступны в любое время суток. Нашим СМИ в Интернете надо работать масштабнее, эффективнее».*

Так, по данным компаний «We AreSocial» и «Hootsuite», отраженным в отчете о состоянии цифровой сферы «GlobalDigital»,в январе 2021 г.во всем мире Интернетом пользовались 4,66 миллиарда человек. Таким образом, уровень проникновения Интернета в мире составляет 59,5%: доступ к нему есть более чем у половины населения земного шара.

В Беларуси уровень проникновения гораздо выше – более 85% жителей нашей страны являются пользователями Интернета.

Социальные медиа (социальные сети и мессенджеры) являются одним из наиболее популярных интернет-ресурсов. В мире насчитывается 4,2 миллиарда их пользователей (53,6% мирового населения). В среднем каждый день в течение 2020 г. в социальных медиа создавалось более 1,3 миллиона новых аккаунтов, что составляет примерно 15,5 новых пользователей в секунду.Таким образом, с каждым годом все больше интернет-пользователей получают информацию, материалы СМИ черезсоциальные сети и мессенджеры.

Рядовой пользователь социальных медиа сейчас проводит на этих платформах 2 часа 25 минут каждый день, что соответствует примерно одному дню в неделю за вычетом времени на сон.

В Беларуси, согласно данным отчета «Digital 2021» и внутренней статистике интернет-платформ, значительная доля трафика белорусов также приходится на мессенджеры и социальные сети.

Интернет позволяет получить быстрый доступ к различного рода информации, быть в курсе последних новостей, оперативно делиться ими со своим окружением. Вместе с тем, качество информации в Интернете не всегда однозначно. Так, нередко в Сети можно встретить непроверенные, а иногда – и целенаправленно искаженные сведения, «фейки». Информационная агрессия на глобальном и национальном уровнях перестает быть редкостью, становясь центральным звеном гибридных войн.

Поэтому очевидно, что сегодня именно контент национальных СМИ и интернет-ресурсов, уровень медиакультуры населения, становятся одними из ключевых факторов, которые обуславливают характер протекания различных социальных процессов в нашей стране. В этой связи Президент Республики Беларусь А.Г.Лукашенко на встрече с политическим активом страны 16 сентября 2020 г. сделал акцент на том, что *«средства массовой информации должны быть проводниками государственной идеологии, а журналисты – самой государственной категорией специалистов».*

Медиапотребление в современном белорусском обществе

Сегодня информация представляет собой один из важнейших ресурсов и, в то же время, одну из движущих сил развития человеческого общества. СМИ, которые эту информацию распространяют, уже давно неформально называют «четвертой властью» ввиду неоспоримости оказываемого ими большого влияния на настроения общества.В связи с этим очень важно понимание места новых технологий в медиапотреблении, осмысление того, какие СМИ используются гражданами, каково их качество и разнообразие.

***Справочно.***

*Медиапотребление – это количественная и качественная оценка медиа-каналов (информационных или развлекательных СМИ), используемых одним человеком или группой людей. В широком смысле сюда относятся чтение газет и журналов, просмотр телепрограмм и прослушивание радио, интернет-активность.*

Современная белорусская аудитория имеет доступ к различным медиа и платформам (телевидение, радио, газеты в онлайн-среде, мобильные приложения, сайты разных СМИ и др.). Медийное поле Республики Беларусь насыщенное и разнообразное. Так, на 1 ноября 2021 г. в Министерстве информации Республики Беларусь зарегистрировано1608 печатных СМИ; 261 телерадиовещательное СМИ;9 информационных агентств; 37 сетевых изданий. При этом большинство из них (1275) –негосударственные (1180 печатных СМИ; 81 – телерадиовещательное; 7 информационных агентств и 7 сетевых изданий).

Информационное пространство нашей страны открыто, несмотря на то, что в этом есть определенные риски: в Беларуси распространяются порядка трех тысяч зарубежных СМИ, большинство – русскоязычных.

Продолжает развиваться Байнет (белорусская часть сети Интернет). Летом 2021 г. в реестре национальной зоны находилось 149 423 домена .BY и .БЕЛ, а за первую половину текущего года в зонах .BY и .БЕЛ было зарегистрировано 1 454 тыс. доменов, или около 87 имен в сутки.

Влияние Интернетана жизнь белорусов колоссально. По данным Национального статистического комитета Республики Беларусь за 2020 г., 85,1% населения в возрасте 6–72 года имеет доступ к Интернету, 71,3% населения выходят в Сеть ежедневно.

Помимо просмотра фильмов, поиска информации и чтения новостей, белорусы активно используют социальные сети и мессенджеры. Этоприводит к тому, что они становятся полноценными коммуникационными центрами. Наиболее популярными мессенджерами у белорусов являютсяViber – 87%, Telegram– 56%, WhatsApp– 46%, Skype – 22%; социальными сетями: ВКонтакте – 3,8 млн пользователей, Instagram– 3,2 млн пользователей, Одноклассники – 2,8 млн пользователей, Facebook– 750 тыс. пользователей.

Процесс обмена информацией в белорусском обществе характеризуется высокой оперативностью и интенсивностью. Активная и повсеместная информатизация позволяет рассматривать новые медиа в качестве влиятельныхисточников информации, оказывающих серьезноевоздействие на формирование общественного мнения. При этом отмечается преобладающая роль социальных сетей и новостных сайтов как информационных источников.

***Справочно.***

*По результатам исследования, проведенного по заказу Министерства информации в 2020 г.Центром социологических и политических исследований БГУ, граждане Беларуси чаще всего обращаются к таким источникам информации, как социальные сети и телевидение (59,8% и 59,4% соответственно). Каждый второй респондент читает информационные и новостные сайты (49,4%), каждый третий использует мессенджеры (34,4%).*

Важным показателем в оценке медиапотребления является первоочередность выбора источника информации в течение дня.Как показывают результаты выше обозначенного исследования, жители регионов Беларуси начинают свой информационный день преимущественно с просмотра телепередач (35,1%) или посещения социальных сетей (33,7%). На третьем месте с существенным отставанием находятся информационные и новостные сайты (14,1%).

Таким образом, доступность Интернета широкой аудитории вывела глобальную сеть в разряд ведущих источников информации.Реалии таковы, что виртуальная среда сегодня стала мощнейшим фактором влияния на население и государство в целом.Как следствие – стремительное развитие данного сегментамедиасредытребует серьезного подхода к решению возникающих в нем проблем.

Правовые основы государственной информационной политики в Республике Беларусь

Растущая роль СМИ (особенно интернет-СМИ) в социальных процессах вызывает необходимость в проведении системной государственной информационной политики, в основе которой лежит фундаментальное право человека на информацию, закрепленное Конституцией Республики Беларусь.

Главным механизмом государственной информационной политики выступает правовое регулирование деятельности СМИ. Государство стремится, с одной стороны, создать благоприятные условия для функционирования масс-медиа, с другой – соблюсти при этом интересы личности, общества и государства.

*«Не умаляя преимуществ, возможностей и перспектив, которые открыл человеку информационный мир, мы должны обратить внимание и на его обратную сторону. На искусственную реальность, которая дала зеленый свет манипуляциям, обману, преступлениям, потворствует низменным инстинктам человека.*

*Постоянное присутствие человека в социальных сетях, на форумах, медиа-каналах формирует интернет-зависимость. Люди просто выпадают из реальной жизни и теряют элементарные коммуникативные навыки. Что еще хуже, они теряют способность к аналитическому мышлению, поскольку содержание и смысл происходящего вокруг формируют за них социальные сети, мессенджеры и поисковые алгоритмы.*

*Происходит это не бесконтрольно. Сознание людей – в руках крупнейших гигантов интернет-индустрии, услугами которых не брезгуют пользоваться спецслужбы отдельных государств»*, – заявил Президент Республики Беларусь А.Г.Лукашенко на VI Всебелорусском народном собрании.

Защита национальных интересов в информационной сфере является одной из важнейших функций государства. В Республике Беларусь до недавнего времени действовали одни из самых либеральных законодательных норм в области работы СМИ, защиты от распространения порочащих сведений и клеветы, защиты персональных данных и национальных интересов в сфере информационной безопасности.

Внешнее вмешательство во внутреннюю политику Беларуси заставляет внимательно посмотреть на законодательный опыт других стран ис учетом имеющейся специфики внедрить его в правовое поле Беларуси.

***Справочно.***

*В Германии в июне 2017 г. был принят закон «О защите прав пользователей в социальных сетях», направленный на цензуру онлайн-экстремизма. Он обязывает социальные сети, у которых больше двух миллионов пользователей в ФРГ, в течение 24 часов с момента получения жалобы удалять посты, содержащие призывы к ненависти и ложную информацию.*

*В апреле 2021 г. Европейский парламент принял закон, требующий от интернет-компаний «удалять или отключать доступ к контенту, помеченному как террористический» в течение одного часа после уведомления национальных властей.*

В этой связи серьезным шагом в защите и развитии белорусского информационного пространства стал ряд новаций, значимых для сферы правоотношений в области массовой информации, предусмотренных в Законе Республики Беларусь от 24.05.2021 № 110-З «Об изменении законов по вопросам средств массовой информации».

Следует отметить, что многие изменения нацелены на регулирование правоотношений в интернет-пространстве.В частности, расширен перечень лиц, которые не вправе выступать в качестве учредителей СМИ. Это касается в том числе и владельцев интернет-ресурсов, в отношении которых приняты решения об ограничении доступа, а также физических и юридических лиц, ранее выступавших в качестве учредителей СМИ, выпуск которого прекращен по решению суда, а также физических и юридических лиц, ранее выступавших в качестве участников или собственников имущества организации, признанной экстремистской.

Также установлен ряд запретов в части создания и функционирования СМИ с иностранным участием. В частности, предусматриваются меры, направленные на минимизацию иностранного влияния на белорусский информационный рынок. Теперь, независимо от времени создания СМИ, их учредителями не могут выступать иностранные юридические лица, иностранные граждане и лица без гражданства, а также юридические лица с иностранным участием.

Расширен перечень информации, распространение которой запрещено как в СМИ, так и на интернет-ресурсах.

***Справочно.***

*В этот перечень, в частности, входит:недостоверная информация; информация, направленная на пропаганду войны, экстремистской деятельности или содержащая призывы к такой деятельности;другая информация, распространение которой способно нанести вред национальным интересам Республики Беларусь или запрещено законодательными актами.*

*Кроме того, введен запрет на размещение результатов опросов общественного мнения, относящихся к общественно-политической ситуации, проведенных без получения необходимой аккредитации.*

*Под запрет подпадает не только размещение подобных материалов, но и гиперссылок на источники, в которых эти материалы содержатся.*

Существенно изменен подход к правовому статусу журналиста СМИ. Так, в целях недопущения распространения «фейковых»новостей запрещено использование прав журналиста СМИ для фальсификации информации, а также распространения недостоверной информации под видом достоверных сведений.

Введена возможность лишения аккредитации журналиста СМИ, если им было совершено умышленное противоправное деяние в процессе осуществления профессиональной деятельности.

Для оперативного пресечения распространения противоправной информацииМинистерство информации, наряду с судом, обладает полномочиями по принятию решения о прекращении выпуска СМИ(например, в случае вынесения двух и более письменных предупреждений юридическому лицу, на которое возложены функции редакции СМИ, либо учредителю СМИ, либо владельцу сетевого издания).

Кроме того, право на вынесение решений об ограничении доступа к интернет-ресурсу, сетевому изданию предоставлено Генеральному прокурору, а также прокурорам областей и г.Минска в отношении интернет-ресурсов, сетевых изданий, посредством которых распространяется информация, направленная на пропаганду экстремистской деятельности или содержащая призывы к такой деятельности, а также информация, распространение которой способно нанести вред национальным интересам Республики Беларусь.

Случаи ограничения доступа к интернет-ресурсам и прекращения выпуска СМИ были дополнены таким основанием, как принятие Межведомственной комиссией по безопасности в информационной сфере решения о наличии информационных сообщений, распространение которых способно нанести вред национальным интересам.

Закрепляется возможность ограничения доступа к копии интернет-ресурса, доступ к которому ранее был ограничен.

***Справочно*.**

*С полным текстом Закона«Об изменении законов по вопросам средств массовой информации»можно ознакомиться по ссылке: https://pravo.by/upload/docs/op/H12100110\_1621890000.pdf.*

Также с целью оперативного противодействия пропаганде экстремизма и распространению экстремистских материалов, в соответствии с постановлением Совета Министров Республики Беларусь от 23.04.2007 № 513 Министерство информации осуществляет ведение и опубликование республиканского списка экстремистских материалов (далее – республиканский список).

***Справочно.***

*К экстремистским материалам относится информационная продукция, используемая для вовлечения в экстремистскую деятельность, и ее пропаганда.*

*Республиканский список размещается на официальном сайте Министерства информации, а также публикуется в газете «Рэспублiка» и сетевом издании «zviazda.by».*

Содержание информационной продукции, включенной в республиканский список, разглашению не подлежит.

Необходимо знать, что распространение, изготовление, хранение, перевозка информационной продукции, содержащей призывы к экстремистской деятельности или пропагандирующей такую деятельность, влечет за собойадминистративную ответственность.

Более того, в рамках реализации постановления Совета Министров № 575 «О мерах противодействия экстремизму и реабилитации нацизма» экстремистскими формированиями признаются в том числе телеграм-каналы, то возможным является применение уголовной ответственности к их участникам, т.е. подписчикам телеграм-каналов.

По данной статье создателям, организаторам и участникам экстремистских формирований грозит лишение свободы на срок до 7 (семи) лет.

Способы противодействия манипулятивным техникам в СМИ

Одним из принципиально значимых направлений в борьбе государства с различного рода манипуляциями в СМИ является предоставление населению объективной, беспристрастной информации о ситуации в стране и мире.

Президент Республики Беларусь А.Г.Лукашенко неоднократно отмечал необходимость активизации работы в Интернете, социальных сетях, создания качественной отечественной медиапродукции, усиленияинформационно-разъяснительной работы в СМИ, в противовес распространению недостоверной информации о Беларуси различными оппозиционными и западными новостными ресурсами.

Для этого в целях своевременного донесения до граждан позиции государства, объективного и всестороннего информирования о деятельности государственных органов Президентом Республики Беларусь был подписан Указ от 19.03.2020 № 106, который внес изменения в Указ от 06.02.2009 № 65 «О совершенствовании работы государственных органов, иных государственных организаций со средствами массовой информации». В соответствии с нимруководители государственных органов и иных организаций несут персональную ответственность за состояние работы по информационному обеспечению и сопровождению государственной политики в медийной сфере.

В то же время, события последних лет неоднократно показывали, что основные сражения за Беларусь сегодня проходят не в высоких кабинетах или в честной борьбе на избирательных участках, а именно в информационном поле. Наша страна и раньше нередко сталкивалась с откровенной провокаторской деятельностью представителей ряда оппозиционных и зарубежных медиа. В погоне за сенсациями отдельные СМИ неоднократно занимались недостоверным освещением событий в Беларуси, стремились при помощи различных «фейков» и искажений реальной информации оправдывать действия организаторов несанкционированных выступлений.

Вырос и градус деструктивных материалов. К сожалению, у пользователей сети Интернет становится все сильнее привычка обращать внимание на острые материалы и пропускать аналитику, кропотливо собранные, интересные, но совсем не сенсационные факты.

Поэтому, с целью противодействия различным деструктивным влияниям и принимая необходимость соответствовать духу времени, в 2020–2021 гг.в отечественном медиапространствебыла развернута широкаяинформационная и разъяснительная работа.

Так, в эфире телеканала «Беларусь 1» центральной площадкой для развенчания и опровержения «фейковых» новостей стала программа «Клуб редакторов». Специальные сюжеты, посвященные данной тематике, выходят в программе «Главный эфир», а в рамках программы «Панорама» имеется регулярная рубрика «Фейку NET». При этом дляподготовки проектов и выпусков новостей используется только официальная информация государственных органов и достоверных источников.

Телеканал «ОНТ» запустил проект «Антифейк», ввел специальные рубрики «Будет дополнено», «Тревожная кнопка». Развенчивание «фейковых» новостейтакже регулярно осуществляется как в рамках информационно-аналитических программ, так и специальных проектов «Марков. Ничего личного» и ток-шоу «ОбъективНО».

На телеканале «СТВ» опровержение «фейков»происходит в информационно-аналитической программе «Неделя», а также в авторских проектах «Тайные пружины политики» и «Политика без галстуков и купюр».

Активно работают в этом направлении БелТА, «СБ. Беларусь сегодня», «Звязда», другие центральные издания.

Так, БелТА систематически публикует материалы по теме противодействия распространению «фейковых» новостей, предлагает своей аудитории авторитетные мнения, высказывания на информационной ленте агентства, сайте belta.by, в еженедельнике «7 дней», журнале «Беларуская думка», а также в аккаунтах агентства в социальных сетях и мессенджерах.

На страницах газет, выпускаемых ИД «Беларусь сегодня», интернет-сайте, в эфире «Альфа-радио» выходят публицистические материалы по актуальным темам А.Муковозчика, В.Гигина, Л.Гладкой и других авторов.

Общая тенденция весьма позитивная: традиционные государственные издания и электронные СМИ буквально за год-два резко прибавили и в итоге стали заметной частью Байнета.

Однако все усилия, предпринимаемые государством по развенчанию ложной и деструктивной информации, будут тщетны, если сами белорусы не будут задумываться о том, что и зачем они читают или смотрят, кому они готовы верить.

Поэтому обязанность каждого ответственного гражданина, патриота своей страны состоит в том, чтобы повысить свою осведомленность о проблеме использованияманипулятивных технологий в СМИ и Интернете, развить навыки распознавания и противодействия им.

Первоочередную помощь в этом может оказать способность отличать «фейковые» новости в Интернете от настоящих. Для этого специалисты дают следующие советы:

Изучите источник новости. Прежде всего, необходимо найти первоисточник – того, кто первым опубликовал эту информацию. Следует попытаться понять, что это за ресурс или человек, каковы их цели? Если это сайт – то можно ли на нем найти данные о дате и месте регистрации, сотрудниках, номера телефонов редакции? Если человек – это реально существующий автор? Можно ли ему доверять? Что о нем пишут в Интернете? Если у статьи нет автора, то это часто делается во избежание ответственности за написанное.

Изучите новость целиком. Не следует судить о новостях только по заголовкам, потому что с целью привлечения внимания аудитории названия «фейковых» статей делаются намеренно сенсационными и вызывающими. Но при внимательном прочтении новости оказывается, что заголовок не соответствует внутреннему содержанию статьи. Обращайте внимание на обманчивые заголовки, мнения, которые представлены как факты, искажения фактов, полностью выдуманные обстоятельства и проигнорированные детали.

Изучите ссылки, указанные в новости. Пройдите по ссылкам, вставленным в статью, и проверьте, действительно ли они соответствуют даннойновости. Выясните – ссылки ведут к надежным, авторитетным источникам или к каким-то сомнительным безымянным сайтам или экстремистским Telegram-каналам?

Проверьте дату выпуска. Актуальна ли данная информация? Проверьте хронологию событий, описываемых в новости. Зачастую старые события перерабатываются и преподносятся как новые, даже если они больше не актуальны.

Оценивайте непредвзято. Помните, что люди больше склонны доверять той информации, которая подтверждает их убеждения, и отрицать те сведения, которые противоречат их мнению. Необходимо стремиться избегать этой ошибки.

Обратитесь к специалистам. Ищите подтверждение экспертов, которые действительно разбираются в освещаемой теме. Проверьте их полномочия, квалификацию, гражданскую позицию, а также предыдущие заявления.

Необходимо помнить, что развитая способность различать «фейковые» новости от настоящих сводит к минимуму вероятность манипуляции мнением человека, подталкивания его к осуществлению незаконных действий.

\*\*\*

В настоящее время информационная сфера приобретает ключевое значение для любого государства и каждого человека. Интересы людей становятся все более разносторонними, возрастает значение коммуникационных технологий, расширяется область их использования населением, увеличивается роль информациив жизни общества.

Однако наряду с этим Республика Беларусь, как и все страны, не может игнорировать принципиально новые риски, связанные с информатизацией: наращивание деструктивных воздействий на общество, манипулирование массовым сознанием, распространение недостоверной информации и пр. Еще в марте 2019 г. на заседании Совета Безопасности Беларуси Глава государства А.Г.Лукашенко подчеркнул, что *«… нарастание в мире конфликтности и отсутствие в данной сфере четких правил поведения превращают эти риски в реальные угрозы конституционным основам и всестороннему развитию любого государства»*.

Именно поэтому сегодня необходима эффективная деятельность государства по обеспечению информационной безопасности. Она должна опираться на разумно выстроенную правовую основу и единое понимание стратегических целей и общих задач. Успешное осуществление этой деятельности невозможно без понимания всеми жителями Республики Беларусь возможностей, потенциала и сопутствующих рисков, которые несет в себе современная информационная среда.

**ОСНОВНЫЕ АСПЕКТЫ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ**

***Советы по защите от киберпреступников***

Вас беспокоит ситуация с киберпреступностью? Понимание того, что такое киберпреступение, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.

**Что такое киберпреступление**

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. Большинство (но не все) киберпреступления совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями. Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры. Киберпреступники редко взламывают компьютеры по причинам, не имеющим отношения к получению прибыли, например, по политическим или личным.

**Типы киберпреступлений**

Вот несколько примеров различных типов киберпреступлений:

Мошенничество с электронной почтой и интернет-мошенничество;

Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);

Кража финансовых данных или данных банковских карт;

Кража и продажа корпоративных данных;

Кибершантаж (требование денег для предотвращения кибератаки);

Атаки программ-вымогателей (тип кибершантажа);

Криптоджекинг (майнингкриптовалюты с использованием чужих ресурсов без ведома их владельцев);

Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций);

Большинство киберпреступлений относится к одной из двух категорий;

Криминальная деятельность, целью которой являются сами компьютеры;

Криминальная деятельность, в которой компьютеры используются для совершения других преступлений.

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью зловредов можно удалять или похищать данные.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании - предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений.

Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры с вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети.

Киберпреступники могут также выполнять так называемую атаку с распределенным отказом в обслуживании (DDos). Она похожа на DoS-атаку, но для ее проведения преступники используют множество скомпрометированных компьютеров.

Также, еще есть третья категория киберпреступлений, когда компьютер используется как соучастник незаконного деяния, например, для хранения на нем украденных данных.

Примеры киберпреступлений

Атаки с использованием вредоносного ПО

Атака с использованием вредоносного ПО - это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО. Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей. К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

**Фишинг**

Фишинговая кампания - это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или безопасность организации, в которой они работают. Сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также могут просить получателя в ответном письме предоставить конфиденциальную информацию.

Другой тип фишинговой кампании известен как целевой фишинг.

Мошенники пытаются обмануть конкретных людей, ставя под угрозу безопасность организации, в которой они работают. В отличие от массовых неперсонифицированныхфишинговых рассылок сообщения для целевого фишинга создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от генерального директора или IT-менеджера.

Распределённые атаки типа «отказ в обслуживании»

Распределенные типа «отказ в обслуживании» (DDoS) - это тип кибератаки, которую злоумышленники используют для взлома системы или сети. Иногда для запуска DDoS-атак используются подключенные устройства IoT (Интернет вещей).

DDoS-атака перегружает систему большим количеством запросов на подключение, которые она рассылает через один из стандартных протоколов связи.

Кибершантажисты могут использовать угрозу DDoS-атаки для получения денег. Кроме того, DDoS запускают в качестве отвлекающего маневра в момент совершения другого типа киберпреступления.

**Как не стать жертвой киберпреступления**

Итак, теперь, когда вы понимаете, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные? Следуйте следующим советам:

**Регулярно обновляйте ПО и операционную систему:** Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.

Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты. Используйте сложные пароли, которые трудно подобрать, и нигде их не записывайте. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сильный пароль. Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений - это вложения в электронных спам-сообщениях. **Никогда не открывайте вложение от неизвестного вам отправителя.**

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, - это вредоносные ссылки в спамовых электронных письмах или других сообщения, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

**Не предоставляйте личную информацию, не убедившись в безопасности канала передачи:** Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.Свяжитесь напрямую с компанией, если вы получили подозрительный запрос**.** Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.Желательно пользоваться, при этом, другим телефоном, потому что злоумышленники могут оставаться на линии: вы будете думать, что набрали номер заново, а они будут отвечать якобы от имени банка или другой организации, с которой, по вашему мнению, вы разговариваете.

**Внимательно проверяйте адреса веб-сайтов, которые вы посещаете:** Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Они выглядят легитимно? Не переходить по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.Если ваш продукт (банковская платежная карта) для обеспечения безопасности в Интернете включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.Внимательно просматривайте свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

**Базовые правила «общения» с телефонными мошенниками:** Телефонное мошенничество было и остается одним из наиболее распространенных способов обмана граждан. Обычно цель — завладеть чужими денежными средствами. Как понять, что на другом конце трубки мошенники, и как реагировать на подобные звонки:

Основное правило: не сообщайте данные.  Это правило даже можно назвать «нулевым» – ни при каких обстоятельствах не сообщайте по телефону свои конфиденциальные данные. Необходимо помнить, что банки и другие легитимные организации никогда не потребуют у вас озвучить код из смс, CVV и так далее. Запрос конфиденциальной информации - самый явный признак мошенничества.

При малейшем подозрении необходимо завершить звонок и перезвонить на официальный телефон той организации, от которой якобы поступил первичный вызов. В случае банка, например, телефон можно найти на обратной стороне карты, либо в личном кабинете онлайн-банкинга. Стоит отметить, что помимо финансовых организаций и силовых организаций, мошенники также любят представляться сотрудниками вашего сотового оператора.

**Задайте контрольный вопрос:** Договоритесь с близкими и родственниками о контрольном слове или коротком вопросе, который позволит удостовериться, что звонит не мошенник. Данная мера может показаться чрезмерной, однако часто мошенники пытаются вывести собеседника из равновесия, говоря о том, что близкому человеку грозит опасность. Мы в любом случае должны иметь «холодную» голову и на 100% быть уверенными в том, что звонит именно тот, кого мы слышим, а не робот или злоумышленник.

**Никаких ссылок:** Не реагируйте на сообщения с незнакомых номеров, в которых указаны ссылки для скачивания стороннего ПО или переход на какие-либо веб-страницы с целью получения, например, выигрыша в лотерее (особенно, если ни в каком конкурсе вы не участвовали) и так далее. Такие действия чреваты установкой на ваш телефон вирусного ПО, а также кражей данных и денежных средств.

**Не переводите деньги:** Следующий совет вытекает из предыдущего, но стоит его выделить отдельно: игнорируйте сообщения от незнакомых номеров с просьбой перевода денежных средств. Мошенники могут написать от лица близких родственников (причем, не факт, что у вас такие родственники вообще есть – мошенники делают массовые рассылки, стремясь попасть в большее количество людей). Выходом опять же будет звонок с уточнением на номер человека, от лица которого действуют мошенники.

**Не перезванивайте:**Не стоит перезванивать по незнакомым номерам (если у вас есть такая возможность). Зачастую можно заметить вызов на телефон, который тут же прерывается. Естественное желание -  перезвонить, чтобы узнать, кто звонил. Однако мошенники часто используют платные номера – если вы перезвоните на такой номер, с вас начнет списываться поминутная оплата.

**Ошибка перевода: свяжитесь с банком:** Если вам приходит смс о зачислении средств, а вы не имеете к этому отношения, есть вероятность мошенничества. В случае с балансом мобильного телефона, у человека, который отправил вам денежную сумму, есть возможность оспорить операцию – если вы самостоятельно переведете деньги обратно, мошенники потом еще раз спишут с вас такую же сумму денег. То же самое касается и банковских переводов – лучше не переводить полученные денежные средства самостоятельно, а обратиться в банк с заявлением об ошибочном зачислении.

**Проверяйте источники:** Так как актуальные новости зачастую становятся еще одним инструментом убеждения у мошенников, всегда стоит перепроверять в официальных источниках информацию, которую сообщает звонящий. Коронавирус для всех является крайне актуальной и острой темой, в связи с чем особо участились случаи мошенничества, связанные с вакцинацией или социальными выплатами.Все эти правила – базовые при общении с мошенниками, но каждый день изобретаются новые способы обмана. Иногда этому способствует развитие технологической базы, которую злоумышленники также берут на вооружение – к примеру, создание «голосового клона», который способен имитировать речь реально существующего человека, тем самым еще больше втираясь в доверие к потенциальной жертве. Технология пока широко не используется из-за сложностей создания дипфейка, однако стоит подготовиться и к такому. Противостояние подобному типу мошенничества аналогично с мерами защиты от обычного, телефонного – при малейших сомнениях нужно сбрасывать звонок и перезванивать самостоятельно.Опасность состоит еще и в том, что злоумышленники используют подмену телефонного номера – у абонента высвечивается номер, вроде как похожий на легитимную организацию (например, начинающийся с +357), но на самом деле это звонок с неизвестного мобильного. Лучше быть наиболее осмотрительным и недоверчивым, чем попасться на удочку мошенников. Украденные суммы ограничиваются лишь только жадностью злоумышленника, поэтому один такой звонок может стать серьезным испытанием. Не забывайте всегда напоминать базовые правила безопасности своим родным и близким, в особенности детям и пожилым людям, так как они наиболее уязвимы.

**ОПЕРАТИВНАЯ ОБСТАНОВКА В ОБЛАСТИ. АКЦИЯ «НЕ ПРОЖИГАЙ СВОЮ ЖИЗНЬ!». ДЕТСКАЯ ШАЛОСТЬ С ОГНЕМ. ЭЛЕКТРОБЕЗОПАСНОСТЬ. ИНФОРМАЦИОННЫЯ КАМПАНИЯ МЧС «БЕЗОПАСНАЯ СТАРОСТЬ». ТОНКИЙ ЛЕД**

За 10 месяцев текущего года в Могилевской области произошло 653 пожара, погибло 82 человека. Травмировано 40 человек. В результате пожаров уничтожено 149 строений, 8 голов скота, 40 единиц техники, 860 тонн грубых кормов. 551 пожар произошел в жилом фонде.

Основными причинами возникновения возгораний стали:

- неосторожное обращение с огнём – 212 пожаров;

-нарушение правил устройства и эксплуатации электрооборудования – 152 пожара;

-нарушение правил устройства и эксплуатации отопительного оборудования и теплогенерирующих установок– 134 пожара;

- детская шалости с огнем – 10 пожаров;

-нарушение правил пожарной безопасности при эксплуатации газовых устройств – 5 пожаров;

-проявление сил природы – 5 пожаров.

I. Какова основная причина пожаров и гибели людей на них? Чтобы ответить на этот вопрос не обязательно быть работником МЧС, достаточно регулярно просматривать прессу и интернет. Практически ежедневно в огне не затушенной сигареты обрываются жизни. Всего в области по причине неосторожного обращения с огнем погибло 65 человек, в том числе из-за неосторожности при курении 57 человек. Усугубляющий фактор – алкоголь. Более 70 % из числа погибших на момент пожара находились в состоянии алкогольного опьянения.

Пример: 25 октября около часа ночи спасателям поступило сообщение о пожаре частного жилого дома в д.Забелышин Хотимского района. По прибытии к месту вызова происходило горение дома открытым пламенем, создалось плотное задымление. Со слов соседей, внутри находится человек. Дом нежилой, не электрифицирован, АПИ не установлен. В доме самовольно периодически проживал гражданин 1972 г.р., не работавший.  Его и его гостя – 49-летнего жителя Климовичского района без признаков жизни обнаружили под обрушившимися конструкциями. В результате пожара уничтожена кровля, повреждено перекрытие и имущество в доме. Причина произошедшего – неосторожное обращение с огнем при курении.

Пример: 2 ноября в 10-13 спасателям поступило сообщение о задымлении на 4-ом этаже пятиэтажного общежития, расположенного по ул. Профсоюзной в Могилеве. Лестничная клетка 4 этажа была наполнена дымом. Оперативно установили источник задымления: горела одна из комнат жилого блока, в которой проживал 54-летний мужчина. Его спасатели в бессознательном состоянии обнаружили на полу и передали медикам. К сожалению, реанимационные действия не помогли. Мужчина погиб.

В результате пожара в комнате повреждены постельные принадлежности. Работниками МЧС из соседних комнат проведена эвакуация 8 человек, в том числе 3 детей. По предварительным данным к трагедии привела не затушенная сигарета.

«Сигаретные пожары» легко предотвратить, соблюдая простое, но очень важное правило: никогда не курить в постели и тушить окурок до последней искры, причем тушить в пепельнице. Забудьте о привычке бросать окурки с окна или балкона. «На всякий пожарный», уходя из дома, закрывайте на балконе окна, чтобы окурок, брошенный соседом сверху, не угодил к вам.

Если в Вашей семье есть курильщик – контролируйте его действия и обязательно установите автономный пожарный извещатель, который вовремя оповестит о пожаре.

II. Для привлечения внимания к проблеме пожаров и гибели людей из-за неосторожного обращения с огнем при курении в ноябре в области проводится республиканская акция «Не прожигай свою жизнь!».

Мероприятия проходят в три этапа:

1-й этап – 1-12 ноября – акция проводилась на промышленных, сельхоз предприятиях и в других организациях, а также в пунктах приема вторсырья. Форма работы креативна и динамична: интеллектуальные игры на тематику ОБЖ, диалоги о наболевшем и нагоревшем, демонстрация видеофильмов.

2-й этап – 15-25 ноября – с акционной миссией спасатели посещают вузы, ссузы (лицеи, колледжи), отделения дневного пребывания при региональных наркологических диспансерах. В программе: тематические конкурсы и дискотеки, открытые диалоги, фестивали КВН, конкурсы миниатюр и т.д. К мероприятиям для лиц, злоупотребляющим спиртными напитками, обязательно привлекаются представители УВД и здравоохранения. Встречи представляют собой профилактические беседы с просмотром тематических видеофильмов и практические занятия на тематических площадках. Для закрепления полученных знаний участникам раздают наглядно-изобразительную продукцию.

3-й этап – 26-30 ноября - финальное мероприятие пройдет в местах массового пребывания людей (открытые площадки, торгово-развлекательные центры, сельские советы и т.д.).

Существенную помощь в профилактике «сигаретных пожаров» окажут СМИ. В эфире радиостанций и на страницах периодических печатных изданий появятся тематические викторины, а телеканалы покажут видеофильм «Жертвы пагубной привычки». В сети интернет пройдет конкурс «Я не курю в постели и тебе не советую» на лучшее видео на тему опасности курения в постели, а в социальных сетях, которые так популярны в кругах студентов, — «Не прожигай свою жизнь».

III. Прописные истины о том, что спички детям не игрушка и что детей без присмотра оставлять нельзя – знает каждый взрослый, вот только не все придерживаются этих правил.

Пример: 29 октября 27-летняя многодетная мать жительница д. Барсуки Климовичского района вместе со старшим сыном отправилась в гости. Дома без присмотра закрытыми в квартире остались трое детей: 2014 и 2017 годов рождения. Около 9 часов вечера, когда привычные игры детям надоели, в их руках оказались спички. Малышам не пришлось их долго искать: они лежали в доступном месте на кухне. Огонь попал на ковер, тление которого заполнило комнату едким дымом. Дети перебежали в соседнюю комнату. Просачивающийся дым, крики и плач малышей услышали соседи и вызвали спасателей. В это время вернулась и мать детей. Она открыла квартиру и вывела малышей на улицу. Благо, никто не пострадал. Дети госпитализированы в учреждение здравоохранения по социальным показаниям. Признаков отравления продуктами горения, а также наличие других повреждений от опасных факторов пожара на момент госпитализации не установлено. В результате пожара повреждено имущество в квартире.

В этом году в области произошло 10 пожаров по причине детской шалости с огнем.

Уважаемые взрослые!

- Никогда не оставляйте малолетних детей без присмотра! Создайте все условия, чтобы спички, бытовые газовые и электрические приборы, бытовая химия и таблетки не стали игрушкой для малышей. Убедитесь, что окна в комнате, где играет ребенок, закрыты.

- Постарайтесь организовать досуг детей таким образом, чтобы они не оставались наедине со своими фантазиями.

- Используйте любой удобный момент для беседы с детьми о силе и опасности огня. В доверительной обстановке постарайтесь привить ребенку основные навыки безопасности жизнедеятельности. Беседы должны обучать, а не запугивать. К таким урокам приступайте с раннего детства.

- Необходимо знать о каждом шаге ребенка, о его друзьях.

- Малолетние дети должны хорошо помнить свое имя, номер телефона, фамилию родителей и место их работы, а также номера телефонов экстренных служб.

- Прежде, чем доверить младшего ребенка старшему, убедитесь еще раз: знает ли он, как вести себя в случае непредвиденной ситуации. Обязательно предупредите соседей или родственников, если по каким-то причинам вы вынуждены оставить их одних.

-У детей обязательно должен быть ключ от входной двери, чтобы в случае опасности покинуть жилье.

- И самое главное: прежде чем требовать от ребенка соблюдения указанных правил, задумайтесь, всегда ли вы выполняете их сами. Ваш личный пример обязательно скажется на поведении ребенка, а значит, и на его безопасности.

IV. На 30 % по сравнению с прошлым годом увеличилось количество пожаров, произошедших по причине нарушения правил пожарной безопасности при устройстве и эксплуатации электрооборудования. По данной причине погибло 7 человек. Огненная стихия зачастую забирает жизни самых уязвимых, одиноких и беззащитных – пенсионеров.

Пример: 14 января жертвой огня стала 90-летняя жительница Кричева. Пожар около полуночи обнаружили соседи, когда огонь уже полностью охватил кровлю. Прибывшими спасателями на полу около двери без признаков жизни была обнаружена пенсионерка. По-видимому, женщина пыталась эвакуироваться, однако опасные факторы пожара оказались сильнее. Огонь не пощадил и жилье: повреждена кровля, перекрытие и имущество. Причина произошедшего – короткое замыкание электропроводки.

Пример: Не пощадил огонь и100-летнюю жительницу д. Пригани-2 Круглянского района. Пожар произошел 31 мая около 9 часов вечера. Хозяйку без признаков жизни обнаружили на диване. Как выяснилось, чтобы пенсионерке было тепло и комфортно, родные приобрели электрогрелку, загорание которой и привело к трагедии.

Во избежание трагедий – с помощью специалистапроверьте исправность электрооборудования и проводки. Не забудьте обезопасить и жилье своих престарелых родных и близких.

-Не применяйте для защиты электросетей и электрооборудования вместо автоматических предохранителей и калиброванных плавких вставок защиту не заводского (кустарного) изготовления (скрутки проволоки, «жучки» и др.).

- Не оклеивайте и не окрашивайте электрические провода и кабели.

- Для исключения возгорания электрооборудования из-за скачков и перепадов напряжения пользуйтесь сетевыми фильтрами.

- Следите за тем, чтобы вилки и розетки не нагревались, ведь это первый признак неисправности или перегрузки сети, что, соответственно, может привести к короткому замыканию.

- Ни в коем случае не пользуйтесь самодельными удлинителями, электронагревательными приборами и электроинструментом.

- Одна из главных «заповедей» безопасности – не оставляйте включенные электроприборы без присмотра.

V.По статистике, 50% от общего числа погибших на пожарах — люди старше 60 лет. В силу своих возрастных и физических особенностей риск оказаться жертвами огненной стихии у них гораздо выше, чем у представителей других категорий. Причины пожаров в домах пенсионеров типичны: неосторожное обращение с огнем, эксплуатация неисправных электроприборов или печного отопления, оставленная без присмотра пища на плите. Потеря бдительности, снижение остроты зрения, слуха, проблемы с памятью – те факторы, которые могут сыграть фатальную роль. Самостоятельно починить печь, электропроводку или установить пожарный извещатель – эти мероприятия не всегда под силу и по карману пожилому человеку. Махнут рукой, мол, на мой век хватит. А хватит ли?

Логично, что обеспечить престарелым родителям безопасность в жилье должны помочь дети и внуки. Но реальность оказывается прозаичнее и суровее: в суете дней они забывают о престарелых родителях или не считают своим долгом обеспечить им полноценную и безопасную старость. А что говорить о пожилых родственниках, которые для многих не так близки, как мама и папа, но при этом тоже нуждаются в помощи?.. Чтобы обратить внимание людей на существующую проблему и напомнить о необходимости контроля за состоянием пожарной безопасности в домах престарелых близких, МЧС разработалоновую информационную кампанию «Безопасная старость», которая стартовала по всей стране 1 ноября.

В ее основе лежат реалистичные образы, которые переносят целевую аудиторию в атмосферу отдыха у бабушки с дедушкой за городом: теплые носки, парное молоко, румяные пирожки. Но в этой идиллии есть и «ложка дегтя» – демонстрация примеров нарушения правил безопасности, которые в домах пенсионеров чаще всего приводят к непоправимому. Главный герой кампании не пенсионер, а работник МЧС. Именно в этом и кроется главная идея: за, казалось бы, некоторой комичностью картинки – спасатель, заменивший в кадре предполагаемую всеми старушку, – прячется важный посыл, который и раскрывается в слоганах. «Мы не сможем угостить Вас парным молоком вместо Вашей бабушки!», «Мы не сможем испечь пирожки вместо Вашей бабушки!», «Мы не сможем связать носки вместо Вашей бабушки!»  Эти фразы в полной мере показывают, что стоит на кону, если продолжить безразлично относиться к состоянию безопасности в домах близких пожилого возраста.

Для максимального распространения информационной кампании МЧС задействует все каналы коммуникации: яркие билборды, тематические видеоролики и аудиореклама.

Присоединяйтесь к информационной кампании МЧС и обеспечьте безопасную и счастливую старость своим близким.

VI. На водоемах скоро появится ледяная кромка. Жажда первой зимней рыбалки, хруст льдинок под ножами ледобура и долгожданная первая рыбка из лунки, все это отодвигает здравый смысл и безопасность на задний план. Результат такой беспечности плачевен: ежегодно в ледяной полынье гибнут люди. В текущем году в Республике при подледной рыбалке погибло 10 человек, жизни 5 человек оборвались при падении в воду со льда. Для того, чтобы не повторять трагических ошибок,необходимо знать: безопасным для человека считается лед толщиной не менее 7 см. Прочность льда можно определить визуально: лед голубого цвета - прочный, белого - прочность его в 2 раза меньше, матово белый или с желтоватым оттенком - ненадежен. В устьях рек и протоках прочность льда ослаблена, непрочен лед и в местах быстрого течения, бьющих ключей и стоковых вод, а также в районах произрастания водной растительности, вблизи деревьев, кустов, камыша. Если температура воздуха выше 0 градусов держится более трех дней, то прочность льда снижается на 25%. Экипированные спасательными жилетами рыбаки полагают, что если и проваляться под лед, то будут защищены. Безусловно, если помощь вовремя подоспеет, это поможет удержаться на плаву и дождаться спасения. Однако, если вовремя не прийти на помощь, существует риск замерзнуть. Специалисты утверждают: при низкой температуре воды человек теряет сознание и начинает замерзать уже через 15—20 минут. И жилет для него не становится палочкой-выручалочкой — он служит лишь ярким ориентиром для спасателей. Самостоятельно плыть к берегу тонущему помешает тяжесть намокшей зимней одежды. Плюс шок и страх…К сожалению, далеко не все это учитывают. Каждый из рыбаков думает, что именно его опасность обойдет стороной. Излишняя самоуверенность может закончится трагедией.

То, чего делать нельзя:

Собираться группами на отдельных участках льда; приближаться к промоинам, трещинам, прорубям на льду; переходить водоем по льду в запрещенных местах; выезжать на лед на мотоциклах, автомобилях вне переправ, а также скатываться на санках, лыжах с крутых берегов на тонкий лед.

Что делать, если Вы провалились в холодную воду:

Не паникуйте, не делайте резких движений, сохраните дыхание.

Раскиньте руки в стороны и постарайтесь зацепиться за кромку льда, придав телу горизонтальное положение.

Попытайтесь осторожно налечь грудью на край льда и забросить одну, а потом и другую ноги на лед.

Если лед выдержал, перекатываясь, медленно ползите в ту сторону, откуда пришли, ведь здесь лед уже проверен на прочность.

Если нужна ваша помощь:

*Стали свидетелем подобной ЧС? В первую очередь оцените обстановку. Подумайте, сможете ли помочь человеку, провалившемуся под лед, самостоятельно. Или лучше позвать кого-то еще? В том случае, если поблизости никого нет, вооружитесь палкой, шестом, веревкой или доской, снимите с себя шарф или куртку, ползите к полынье, равномерно распределяя вес вашего тела по поверхности и толкая спасательное средство перед собой. Приблизившись на максимально возможное расстояние, не ближе 3—4 метров, протяните тонущему палку или веревку (одежду). Когда начнете вытаскивать пострадавшего, попросите его работать ногами, так будет значительно легче справиться. Оказавшись вместе со спасенным человеком в безопасности, вызовите «скорую помощь».*

Под особый контроль - безопасность детей! Объясните детям, какую опасность таит в себе коварный лед, что ни в коем случае нельзя играть на нем и переходить водоем, используя лед в качестве моста. Не допускайте, чтобы дети находились без присмотра вблизи рек, прудов, карьеров. Не разрешайте им кататься на санках, лыжах, коньках по замерзшим водоемам.