МАТЕРИАЛЫ

для информационно-пропагандистских групп

(май 2021 г.)

1. **ОСНОВНЫЕ АСПЕКТЫ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ**

*Материал подготовлен*

*Академией управления при Президенте Республики Беларусь на основе сведений*

*Следственного комитета Республики Беларусь, Министерства внутренних дел Республики Беларусь, информационного агентства «БелТА»*

В настоящее время Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека.   
С одной стороны, это открывает перед белорусскими гражданами и обществом ряд перспектив, с другой – влечет появление новых рисков и угроз. Так, бурное развитие телекоммуникационных технологий, стремительный рост числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к увеличению количества киберпреступлений.

Беларусь, как и другие государства, не может игнорировать принципиально новые риски, связанные с проистекающей информатизацией. Как отметил в ходе VI Всебелорусского народного собрания Президент Республики Беларусь А.Г.Лукашенко, «не умаляя преимуществ, возможностей и перспектив, которые открыл человеку информационный мир, мы должны обратить внимание на его обратную сторону. Искусственную реальность, которая дала зеленый свет манипуляциям, обману, преступлениям, потворствует низменным инстинктам человека».

Вопросы цифровой трансформации преступности сегодня являются одними из наиболее злободневных. И от того, насколько эффективно удастся противостоять этому вызову, зависит не только защищенность прав и интересов граждан, но и информационная безопасность общества и государства. При этом универсальных подходов, позволяющих эффективно противодействовать высокотехнологичным преступлениям, не выработано ни одним государством мира.

*Несмотря на принимаемые меры, на протяжении последних лет в Республике Беларусь наблюдается устойчивый рост количества регистрируемых киберпреступлений: в 2015 году – 2 440 преступлений, в 2016 – 2 471, в 2017 – 3 099, в 2018 – 4 741, в 2019 – 10 539,  
в 2020 – 25 561.*

*Изучение международного опыта показывает, что увеличение числа киберпреступлений свойственно большинству государств мира. К примеру, в Российской Федерации число таких уголовно наказуемых деяний в 2020 году выросло на 73,4%, а их удельный вес в структуре преступности составил 25%.*

Среди **факторов, стимулирующих рост киберпреступлений**, можно выделить следующие.

**Опережающие темпы освоения сети Интернет в Республике Беларусь**. Так, в 2020 году доля населения нашей страны, пользующегося Интернетом, составила 85,1%; по плотности проникновения широкополосного доступа в сеть Интернет Беларусь вышла на среднеевропейские показатели, а по скорости – на передовые позиции в мире.

**Уровень компьютерной грамотности граждан недостаточно высок, отстает от скорости внедрения тех или иных компьютерных систем в повседневную жизнь**. Кроме того, многие граждане недостаточно ответственно относятся к защите и безопасности собственной информации и личных данных.

**Ускоренный** **переход многих сфер общественных отношений, включая товарный и денежный обороты, в интернет-пространство,** вызванный распространением коронавирусной инфекции Covid-19.

Развитие дистанционных способов совершения преступлений, при которых отсутствует прямой контакт между злоумышленниками и их жертвами, привело к тому, что киберпреступления ушли из физической реальности в онлайн-пространство. В целях противодействия данным правонарушениям, 26 марта 2021 г. в Республике Беларусь был утвержден Комплексный план мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021–2022 годы.

В настоящее время при характеристике компьютерных преступлений используется целый ряд понятий: «информационное преступление», «киберпреступление», «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий», «виртуальное преступление».

Согласно действующему законодательству Республики Беларусь, в содержание понятия «компьютерная преступность» включают:

1) преступления против информационной безопасности (модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

2) хищения путем использования средств компьютерной техники;

3) изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнего;

4) иные преступления, так или иначе связанные с использованием компьютерной техники: доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет; разглашение врачебной тайны; незаконное собирание либо распространение информации о частной жизни; клевета; оскорбление; распространение ложной информации о товарах и услугах; заведомо ложное сообщение об опасности; шпионаж; умышленное либо по неосторожности разглашение государственной тайны; умышленное разглашение служебной тайны и др.

Таким образом, **к компьютерным преступлениям относятся** правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

*В 2020 году в Республике Беларусь всего было зарегистрировано 95 тыс. преступлений, из них более 25 тыс. – это компьютерные преступления (92% от которых составляли хищения). В то же время еще в 2014 году их численность составляла всего 2,3 тыс.,* т.е. ***наблюдается рост подобных преступлений более чем в 10 раз.***

***В чем состоит цель киберпреступников?***

Как правило, киберпреступники выдают себя за людей из действующих на законных основаниях организаций и учреждений, **чтобы обманом вынудить граждан раскрыть личную информацию и предоставить преступникам деньги, товары и/или услуги**.

Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные, имущество и денежные средства граждан.

***Какие виды киберпреступлений***

***выделяют в отношении граждан?***

Наиболее распространенным видом проявления киберпреступности является **хищение денежных средств с карт-счетов граждан**. Причем в большинстве случаев эти преступления становятся возможны в результате беспечных действий самих потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

*За первые месяцы 2021 года уже зафиксирован рост количества хищений с банковских карточек белорусов более чем на 270% по сравнению с этим же периодом 2020 года.*

Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих способов:

1. *«Фишинг».* Этот неофициальный термин происходит от английского «fishing» («рыбная ловля»). В качестве своеобразной «удочки» преступники используют специально созданный интернет-сайт с формой ввода на нем реквизитов доступа к банковскому счету, а в качестве «наживки» – некий сообщенный потерпевшему предлог для перехода на этот сайт и заполнения платежных реквизитов.

Например, преступник отслеживает на интернет-сайте kufar.by свежие объявления о продаже чего-либо. Просмотрев абонентский номер автора объявления, находит его в одном из мессенджеров (Viber, Telegram, WhatsApp) и вступает в переписку, якобы желая купить выставленный на продажу предмет. Затем пересылает в мессенджере ссылку на поддельную страницу предоплаты, где продавцу нужно ввести реквизиты своей карты для того, чтобы получить деньги от покупателя. При переходе по гиперссылке невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных сервисов (Куфар, ЕРИП, CDEK, Белпочта, сайты различных банков и др.). Адрес поддельной веб-страницы также может напоминать реальный (kufar-dostavka.by, erip-online.com, belarusbank24.xyz, cdek-zakaz.info и др.). Если жертва «попадется на удочку» и заполнит форму, соответствующие реквизиты доступа к банковскому счету окажутся у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета или электронные кошельки, зарегистрированные на подставных лиц.

Гиперссылки на фишинговые сайты могут пересылаться не только в ходе переписки в мессенджерах, но и при общении в социальных сетях, а также размещаться на других сайтах, якобы что-то продающих или покупающих.

**В последнее время участились случаи создания фишинговых сайтов, ориентированных под запросы пользователей в поисковых системах**. Граждане попадают на них прямо из Google и Яндекса после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет банкинг» и т.д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска, но не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения, потерпевший заполняет открывшуюся форму авторизации, данные которой отправляются не банку, а преступнику.

1. *«Помощь другу».* Данный способ преступлений был наиболее распространен в 2017–2019 годах, но не потерял своей актуальности и сегодня. Сначала преступники путем подбора пароля или фишинга осуществляют несанкционированный доступ («взлом») к страницам социальных сетей (в основном – «ВКонтакте»). После этого иным пользователям, добавленным в раздел «Друзья» взломанной страницы, рассылаются сообщения с просьбой предоставить фотографию или данные банковской платежной карты под различными предлогами, например, чтобы срочно сделать какой-то безналичный платеж, так как карточка обратившегося якобы заблокирована. Также злоумышленник, скрывающийся под именем друга, может просить перевести ему на карту определенную сумму денег в связи с внезапным попаданием в сложную жизненную ситуацию. Доверчивый пользователь, полагая, что общается с настоящим владельцем страницы, переводит деньги либо сообщает преступнику реквизиты своей банковской карты (а зачастую – и код безопасности, высылаемый в SMS-сообщении банковским учреждением), после чего с его карт-счета похищаются денежные средства.

*Еще одним видом мошенничества в социальных сетях, связанным с помощью другим людям, является* ***деятельность фальшивых благотворительных фондов, которые осуществляют сбор денег на лечение****. В таких случаях мошенники создают группу и распространяют информацию о том, что якобы нужны средства для лечения тяжелобольного человека (особенно часто – ребенка).* ***Чтобы не попасться на удочку мошенников, необходимо всегда запрашивать документы и дополнительные сведения****.*

1. *«Вишинг»* происходит от английского «voice fishing» («голосовой фишинг» или «голосовая рыбная ловля»). Данный способ выражается в осуществлении звонка на абонентский номер потерпевшего или в его аккаунт в мессенджере (в основном, это Viber или Telegram). В ходе голосового общения преступник представляется работником банка или правоохранительного органа (МВД, КГБ, Следственного комитета) и под вымышленным предлогом (пресечение подозрительной транзакции, повышение уровня безопасности пользования картой, перепроверка паспортных данных владельца банковского счета и т.д.) выясняет у потерпевшего сведения о наличии банковских платежных карточек, сроках их действия, CVV-кодах (трехзначный код на обратной стороне карты), паспортных данных, SMS-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты банковских платежных карточек, а также анкетные данные лиц, на имя которых они выпущены.

В большинстве случаев при совершении звонков преступники используют IP-телефонию.

Последствия использования злоумышленниками подобного способа мошенничества бывают весьма печальными.

1. *Свободный доступ к банковской карте*. Не всегда для хищения с банковских счетов используются хитрые схемы. В ряде случаев причинами этого становятся утеря банковских карт, оставление их в легкодоступном месте, их передача иным лицам для осуществления разовых платежей. При этом увеличивает риск остаться без заработанных денежных средств хранение PIN-кода рядом с картой (например, записанным на бумажке в кошельке или на самой банковской карте).

Разновидностью подобного легкомыслия является хранение фотоизображений банковских карт или платежных реквизитов в памяти мобильного телефона, в почтовом аккаунте или дистанционном облачном хранилище. При несанкционированном доступе к такому хранилищу преступник получает и беспрепятственный доступ к банковскому счету его владельца.

1. *Покупка с предоплатой*. Наиболее примитивной, но от этого не менее работающей формой интернет-мошенничества является размещение преступниками на виртуальных досках объявлений, тематических сайтах, в социальных сетях, группах интернет-мессенджеров объявлений о продаже каких-либо товаров по «бросовым» ценам. Но для получения товара (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту или электронный кошелек. Правда, после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.
2. *Шантаж*. В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. Например, получив несанкционированный доступ к Интернет-ресурсам (страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам) и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет.
3. *Иные мошенничества*. Также можно выделить еще несколько типов мошенничества, которые в недавнем прошлом зачастую успешно использовались на территории Республики Беларусь:

* Просьбы пополнить счет определенного номера мобильного телефона или платежной карты в виде: «Мама, пополни счет на 20 рублей. Мне не перезванивай – позже перезвоню. Нужно срочно!».
* Звонок с номера друга или родственника, в котором собеседник утверждает, что он сотрудник правоохранительных органов, просит вознаграждение, обещая предотвратить возбуждение уголовного дела в отношении близкого человека.
* Когда мошенник звонит и сразу отменяет вызов. Перезвонив на отобразившийся номер, абонент слышит автоответчик или гудки, в это время со счета его мобильного телефона списываются деньги, так как вызов совершается с применением переадресации на платный номер.
* Когда приходит SMS-сообщение о некоем выигрыше, после чего абоненту предлагают отправить платное сообщение в ответ или отправить небольшую сумму на банковскую карту для получения «лжевыигрыша».
* Когда приходит SMS-сообщение с гиперссылкой, пройдя по которой пользователь запускает процесс скачивания вируса.
* Когда поступает звонок от «представителя сотового оператора», во время которого злоумышленники предлагают перерегистрировать SIM-карту. При этом пользователь вводит специальный код или отправляет SMS-сообщение, после чего с баланса его мобильного телефона списываются деньги.
* Когда приходит SMS-сообщение или поступает звонок, в ходе которого сообщается, что абонент не оплатил штраф. После этого человеку предлагается произвести его оплату, перечислив деньги на «специальный» расчетный счет или пополнив банковский счет.
* Когда приходит SMS-сообщение с информацией о том, что платежная карта заблокирована, и указывается номер, по которому можно получить справку или помощь. После звонка у абонента запрашивают PIN-код, CVV-код (трехзначный код на обратной стороне карты), номер карты и другие данные, необходимые для снятия денег с банковского счета.

***Какие способы мошенничества бывают в отношении юридических лиц и индивидуальных предпринимателей?***

Киберпреступления причиняют ущерб не только гражданам. Часто действия злоумышленников направлены на завладение денежными средствами **юридических лиц (предприятий, учреждений и организаций) и индивидуальных предпринимателей**. Но и здесь главным условием, дающим возможность совершения подобных злодеяний, является «человеческий фактор», т.е. грубые ошибки, допускаемые работниками: от руководителей до секретарей, бухгалтеров и менеджеров. Все чаще потерпевшими становятся те юридические лица и индивидуальные предприниматели, которые осуществляют свою деятельность при помощи зарубежных контрагентов.

Среди наиболее типичных форм посягательств хакеров на денежные средства и охраняемую информацию юридических лиц являются ***BEC-атаки*** (от английского: «business email compromise» – компрометация бизнес-переписки).

Реализация подобной схемы хищения возможна посредством получения несанкционированного доступа к электронной почте одной из сторон сделки. В этой ситуации злоумышленники обладают информацией о предмете, условиях договора и могут вести переписку, не вызывая подозрения (в случае необходимости ими направляются дополнительное соглашение, счет-проформа (инвойс) с измененными реквизитами банковского счета и контактными данными представителей фирмы путем их «наложения» на подготовленные ранее и сохраненные в сообщениях документы).

Кроме того, имеются случаи, когда от имени белорусских субъектов хозяйствования после взлома их корпоративной почты в адрес зарубежных партнеров также направлялись письма, счета-проформы с измененными банковскими реквизитами. В результате денежные средства, причитающиеся белорусским предприятиям за произведенную (поставленную) продукцию, переводились на счета мошенников.

Также возможна ситуация, когда после согласования существенных условий контракта с зарубежным партнером, а в отдельных случаях и его подписания, на электронную почту организации (предприятия) преступниками направляется сообщение якобы от имени сотрудника иностранного контрагента об изменении реквизитов обслуживающего банка и необходимости перечисления денежных средств на новый счет. При этом адрес электронной почты мошенников имеет существенное сходство с реальным, что зачастую остается незамеченным. Последующая переписка уже осуществляется с киберпреступниками. Далее под предлогом оплаты товаров иностранных компаний и вследствие предоставления по электронной почте ложных банковских реквизитов на счета мошенников перечисляются денежные средства со стороны субъектов хозяйствования как государственного, так и частного сектора экономики.

***Как не стать жертвой киберпреступления?***

1. **Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт**, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

**ВНИМАНИЕ:** *помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp)*.

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, **обязательно проверяя доменное имя ресурса в адресной строке браузера**.

3. **Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам**; это же относится к фотографиям и иным видам информации конфиденциального характера.

4. Следует **воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги**, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

5. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт **по просьбе пользователей сети Интернет**.

6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам **необходимо использовать сложные пароли, исключающие возможность их подбора**. Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).

7. При составлении платежных документов **важно проверять платежные реквизиты получателя денежных средств**.

8. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек **не следует отвечать на подобные сообщения, а необходимо связаться с данными пользователями напрямую посредством иных средств связи**.

9. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

10. **Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров**; не переходить по ссылкам в сообщениях о призах и выигрышах.

11. Необходимо **использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу** не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

12. Следует **ознакомить с перечисленными правилами безопасности своих родственников и знакомых**, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

***Какие советы можно дать юридическим лицам, чтобы обезопасить себя от мошенничества?***

1. **Выработать четкий план реагирования** и ознакомить работников с перечнем сведений, относящихся к коммерческой, служебной и иной тайне.
2. **Исключить в своей деятельности использование бесплатных почтовых сервисов**, а также **принимать дополнительные меры защиты корпоративной электронной почты** (подключение двухфакторной аутентификации, соблюдение требований к сложности пароля и периодичности его смены, использование антивирусного программного обеспечения).
3. Неукоснительно **соблюдать правила пользования системой дистанционного банковского обслуживания**.
4. **Создавать резервные копии данных** и хранить их на съемных носителях.
5. **Проверять правильность адреса электронной почты контрагента при получении и отправке сообщений**, а также **поддерживать контакт с его представителем** и **согласовывать ключевые вопросы** дополнительно посредством иных средств связи (телефонных переговоров, использования факсимильной связи, мессенджеров и пр.).
6. **Не использовать рабочие устройства в личных целях,** а служебные ящики электронной почты – для регистрации на торговых и развлекательных онлайн-площадках.
7. **Наладить строгий действенный контроль за соблюдением утвержденных мер информационной безопасности** (соответствие программного обеспечения, проверка отсутствия несанкционированного доступа к внешним информационным ресурсам и т.д.).

Современный мир характеризуется динамичными глобальными процессами. Совершенствование информационной сферы и обеспечение ее безопасности становится одним из ключевых моментов, влияющих на общественное и государственное развитие Республики Беларусь.

В этой связи в нашей стране уделяется повышенное внимание обеспечению защищенности информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. В частности, ответные векторы государственной политики обозначены в утвержденной 18 марта 2019 г. Концепции информационной безопасности Республики Беларусь. В то же время, как отметил Президент Республики Беларусь А.Г.Лукашенко в ходе VI Всебелорусского народного собрания, нужно не только более активно выявлять и пресекать экстремистскую, мошенническую и иную незаконную деятельность, но и активно работать над повышением информационной грамотности населения.

1. **ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ И ЗАНЯТОСТИ ДЕТЕЙ В ЛЕТНЕЕ ВРЕМЯ**

В нашей стране ежегодно констатируются факты гибели и травматизма детей. Несмотря на большое разнообразие травм у детей, причины, вызывающие их, типичны. Прежде всего, это халатность, недосмотр взрослых, неосторожное, неправильное поведение ребенка в быту, на улице, во время игр. Поэтому одна из основных задач родителей – предупреждение детского травматизма:

* устранение травмоопасных ситуаций;
* систематическое привитие навыков безопасного поведения.

**ОТРАВЛЕНИЯ, ПРОГЛАТЫВАНИЕ ИНОРОДНЫХ ПРЕДМЕТОВ**

Достаточно часто среди детей регистрируются отравления, причинами которых становятся небрежно хранящиеся лекарственные вещества и средства бытовой химии. Известны случаи, когда во время игр дети случайно проглатывали не только опасные вещества, но и мелкие предметы – батарейки, монеты, пуговицы. Как правило, это происходит непроизвольно – ведь малыши стараются всё попробовать на вкус.

|  |
| --- |
| **Как предотвратить подобные случаи:**  - храните лекарства и химические вещества в местах, недоступных для детей;  - не давайте маленьким детям те игрушки, которые не предусмотрены для их возраста.;  - не используйте предметы быта для развлечения или отвлечения детей;  - не оставляйте детей без присмотра! |

**ОЖОГИ, НЕОСТОРОЖНОЕ ОБРАЩЕНИЕ С ЛВЖ**

Исходя из характера случаев получения ожогов детьми в быту, следует отметить, что в каждом из них травмирования можно было бы избежать при надлежащем контроле взрослых.

Как показывает практика, дети могут получить серьезные травмы из-за неосторожности при использовании легковоспламеняющихся жидкостей. Вспышки паров бензина, ацетона, бензола, толуола, некоторых спиртов и эфиров периодически становятся причиной возгораний, в результате которых дети попадают в больницу.

|  |
| --- |
| **Профилактика:**  - не разрешайте детям самостоятельно разжигать отопительные печи и мангалы;  - обязательно расскажите об опасности легковоспламеняющихся жидкостей;  - не используйте сами легковоспламеняющиеся и горючие жидкости при разведении костров, приготовлении пищи на огне; |

**ОКНА**

Особенно часто о трагических случаях, связанных с падением малышей из окон или с крыш, можно услышать в конце весны, летом и в начале осени. Происходит это по разным причинам: родители отвлеклись или вовсе отсутствовали дома, дети играли или опирались на москитные сетки, не выдержали стеклопакеты .

|  |
| --- |
| **Чтобы избежать случаев выпадения из окон:**  - установите блокираторы открывания окон либо специальные фиксаторы, которые не позволяют ребенку открыть окно более, чем на несколько дюймов;  - используйте ограничители открывания окон со стальным тросом, которые позволят открыть окно только на длину троса;  - защитите окна, вставив оконные решетки;  - оборудуйте окна специальными накладными ручками на замке с комплектом ключей;  - отодвиньте от окон все виды мебели и не оставляйте в комнате детские стульчики и табуретки;  - не устанавливайте москитную сетку – ребенок воспринимает ее как преграду и опирается;  - не оставляйте окна открытыми настежь, если в квартире ребенок;  - не позволяйте ребенку играть на подоконнике. |

**ЛЮКИ, ЯМЫ, КОЛОДЦЫ, ОБРУШЕНИЕ ГРУНТА**

Отсутствие порядка в содержании домового хозяйства, а также на городских улицах представляют особую опасность провалиться туда и получить серьезную травму. Для ребёнка падение в люк канализационного колодца может закончиться летальным исходом. Помимо возможного смертельного удара по голове падающей крышкой, ребёнок может утонуть или задохнуться в магистральной канализационной трубе.

Часто дети выбирают для игр замороженные стройки, пустующие котлованы и заброшенные карьеры. Ведь ребятне нравится играть с песком, и они не понимают той опасности, которая им угрожает. Дети строят лазы и копают траншеи, делают лабиринты и пещеры в песке, скатываются со склона или карабкаются наверх по песчаной горке. Но песок очень опасный, ведь обрушение грунта происходит моментально, и возможности выбраться из-под завала практически нет.

|  |
| --- |
| **На что следует обратить внимание для обеспечения безопасности ребенка?**  - расскажите ребенку об опасности люков;  - объясните своим детям, что нельзя заходить на территорию карьеров, а тем более там играть, рыть в склонах котлованов подземные ходы, прыгать с откосов. |

**ВОДА**

Основное количество несчастных случаев на воде приходится на теплый период года. Открытые водоемы, безусловно, источник опасности, и поэтому осторожность при купании и плавании вполне оправдана. Основными причинами несчастных случаев на воде с участием детей, как правило, являются недостаточный контроль со стороны родителей, незнание правил безопасного поведения и неумение плавать.

|  |
| --- |
| **Для предотвращения несчастных случаев на воде:**  - не оставляйте детей без присмотра вблизи водоемов, даже если ребенок отлично плавает;  - запретите ребенку нырять с ограждений или берега;  - расскажите об опасности игр на воде;  - помните, особую опасность для малолетних детей представляют любые емкости с водой (ванны, бочки, бассейны, ведра и др.). |

**ЖЕЛЕЗНАЯ ДОРОГА**

Каждому из нас приходится сталкиваться с железной дорогой: одним чаще, другим реже, часть учеников пользуются железнодорожным транспортом, или пересекают железнодорожные пути при следовании в школу, на тренировку и т.д. Часть детей ищут приключения, причем в самых неподходящих для таких забав местах.

|  |
| --- |
| **Объясните ребенку, что нельзя:**  - перебегать железнодорожные пути перед приближающимся поездом;  - подлезать под платформу и подвижной состав;  - играть вблизи железнодорожных путей;  - кататься на кабинах и крышах поездов;  - класть на пути посторонние предметы  - переходить железнодорожные пути в неустановленных местах;  - пользоваться вблизи железнодорожного полотна наушниками и разговаривать по сотовому телефону. |

**ДЕТСКАЯ ШАЛОСТЬ С ОГНЕМ**

Пожары, возникающие по причине детской шалости с огнем – явление, к сожалению, далеко не редкое. Финал таких пожаров может быть очень трагичным. Почти все дети проявляют повышенный интерес к огню, не осознавая в полной мере его потенциальную опасность.

|  |
| --- |
| **Предотвратите детскую шалость с огнем:**  - научите ребенка действиям при пожаре, покажите ему возможные выходы для эвакуации;  - научите ребенка не паниковать и не прятаться в случае пожара;  - не доверяйте детям следить за электроприборами, печами и газовой плитой;  - прячьте от ребенка спички, зажигалки, бытовую химию и др.;  - не оставляйте малолетних детей без присмотра! |

**ЭЛЕКТРОТРАВМЫ**

Электричество окружает нас повсюду, облегчая жизнь, а неисправности в нем случаются редко, да и обычно причиняют мало вреда. Но, до определенной поры. Ведь без соблюдения правил пользования электроприборами возможно поражение электрическим током.

|  |
| --- |
| **Как предотвратить подобные случаи:**  - помните: электрические устройства, которые контактируют с человеком, должны быть тщательно изолированы и заземлены;  - защитные устройства на штепсельные розетки снижают риск электротравмы в домах с маленькими детьми;  - регулярно проверяйте бытовую технику на предмет повреждений;  **- объясните детям, что нельзя** пользоваться электроприборами без разрешения взрослых. |

Рассматривая каждый случай гибели ребенка, понимаешь, что трагедиям сопутствовали обыкновенные житейские обстоятельства – родители ушли на работу, в магазин, к соседям, или занимались во дворе хозяйственными делами. Другими словами, дети оставались без присмотра. А далее непоправимый и жестокий итог родительской безответственности ‑ гибель ребенка. За оставление ребенка в опасности предусмотрена уголовная ответственность в соответствии со ст. 159 УК Республики Беларусь.

**Информация**

**о занятости детей в летнее время.**

1. Планируется открыть всего 24 РВО с охватом 299 учащихся.

РВО на базе учреждений общего среднего образования: СШ № 1 г.п. Шумилино; СШ № 2 г.п. Шумилино; Обольская СШ; Никитихинская СШ; Башневская БШ; Мишневичская я/с-БШ; Кордонская СШ; Слободская я/с-БШ; Амбросовичская я/с-БШ; «Мишковская я/с-начальная школа»;

- по месту жительства учащихся: д.Язвино (спортплощадка); д.Суровни (спортплощадка); д.Сиротино на базе Сиротинского сельского дома культуры; д. Лежни на базе Лежневского сельского клуба; а/г Кривое Село на базе библиотеки; д.Приозёрная (здание начальной школы); д. Победа на базе сельской библиотеки, д. Грудиново (сельский дом культуры), д.Леоново (территория старой школы), д.Добрино на базе сельской библиотеки.

2. В ГУДО «Шумилинский РЦДиМ» будут работать объединения по интересам:

|  |  |  |  |
| --- | --- | --- | --- |
| Месяц | Количество объединений по интересам | Количество в них детей | В том числе  спортивные |
| Июнь | 47 | 451 | 4(48) |
| Июль | 35 | 340 | 4(48) |
| Август | 47 | 451 | 4 (48) |

В СШ №1 в летний период будет проводиться секция «Футбол», в Амбросовичской я/с-БШ будет работать объединение по интересам «Фантазия» и спортивная секция по УФП. В июне месяце в Слободской я/с-БШ будут работать секция «Спортивные игры», объединения по интересам «Экознайка», «Пропильная резьба и выжигание по древесине». В Никитихинской СШ в июле месяце будет проходить секция по ОФП, в июне-июле – объединения по интересам «Юный информатик», «Юный эколог», «Художественная вышивка».

**Оздоровление детей в летний период.**

Представительство Витебское областное управление Республиканского центра по оздоровлению и санаторно-курортному лечению населения Шумилинского района (далее – Представительство) информирует:

согласно Плана распределения путевок на санаторно-курортное лечение населения, за счет средств государственного социального страхования, будет выделено Шумилинскому району 54 путевки для детей на 2021 год.

согласно п.7 Указа Президента Республики Беларусь от 28.08.2006 г. № 542 «О санаторно-курортном лечении и оздоровлении населения»

несовершеннолетние дети имеют право на бесплатное санаторно-курортное лечение и оздоровление. Для получения детских путевок на санаторно-курортное лечение и оздоровление от Представительства председателем комиссии по оздоровлению и санаторно-курортному лечению детей работников организации (предприятия, учреждения), с учётом того, что организация стоит на обслуживании в Представительстве, направляется заявка на детские путевки не позднее 56 дней до начала квартала. Представительством путевки выделяются, согласно Плана распределения путевок на санаторно-курортное лечение и оздоровление в соответствии с количеством работающих в организации (предприятии, учреждении).

1. **ВСЕМИРНЫЙ ДЕНЬ БЕЗ ТАБАКА 2021 ГОДА**

Всемирный день без табака отмечается ежегодно 31 мая, начиная с 1987 года, по инициативе ВОЗ. Кампания направлена на привлечение внимания мировой общественности к связанным с употреблением табака рискам для здоровья и к эффективным мерам политики по снижению уровней потребления табака.

В 2021 году ВОЗ запустила глобальную кампанию по случаю Всемирного дня без табака – 2021, которая будет проходить в течение всего года под лозунгом «Пора отказаться от табака».

В условиях пандемии COVID-19 отказаться от табака может быть не так просто, особенно с учетом дополнительного стресса из-за вызванных пандемией социальных и экономических трудностей.

Табак убивает до половины употребляющих его людей. Каждые 6 секунд из-за табака умирает примерно один человек. Ежегодно табак приводит почти к 6 миллионам случаев смерти, из которых более 5 миллионов случаев происходит среди потребителей и бывших потребителей табака, и более 600 000 — среди некурящих людей, подвергающихся воздействию вторичного табачного дыма.

Табакокурение – агрессивный фактор риска сердечно-сосудистых заболеваний. Риск смерти от [инфаркта миокарда](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%B0%D1%80%D0%BA%D1%82_%D0%BC%D0%B8%D0%BE%D0%BA%D0%B0%D1%80%D0%B4%D0%B0) и инсульта у курящих в 2-4 раза выше, чем у некурящих. Каждый седьмой курильщик сталкивается с заболеванием, поражающим сосуды нижних конечностей.

Сигаретный дым, попадая в легкие, значительно увеличивает риск развития пневмонии, эмфиземы, хронического бронхита и других легочных заболеваний.

Курение табака является канцерогенным для человека и приводит к развитию онкологических заболеваний.

Отказ от табака приносит пользу здоровью как сразу, так и в долгосрочной перспективе. Всего через 20 минут после прекращения курения замедляется пульс. В течение 12 часов содержание угарного газа в крови снижается до нормального уровня. В течение 2–12 недель улучшаются кровообращение и функция легких. В течение 1–9 месяцев постепенно пропадают кашель и одышка.

С целью защиты нынешнего и будущих поколений от разрушительных последствий потребления табачных изделий для здоровья, снижения социальных, экологических и экономических последствий потребления табака и воздействия табачного дыма в республике проводится активная работа по профилактике табакокурения. 27 июля 2019 года вступил в силу [Декрет](http://pravo.by/document/?guid=12551&p0=Pd1900002&p1=1&p5=0) № 2 «Об изменении декретов Президента Республики Беларусь», предусматривающий корректировку декретов от 17 декабря 2002 года № 28 и от 18 октября 2007 года № 4, ужесточающий антитабачное законодательство.

Основной целью Декрета являются последовательное ограничение доступности табачных изделий, предотвращение негативного влияния курения на состояние здоровья населения. Декретом предусмотрено законодательное урегулирование производства, оборота и использования электронных систем курения, а также устройств, используемых для нагревания табака без его горения или тления – систем для потребления табака.

Введен запрет открытой выкладки жидкостей для электронных систем курения в витринах и ином торговом оборудовании. Предусмотрены ограничения по местам продажи, использования (потребления) электронных систем курения. Введены запреты на рекламу, продажу несовершеннолетним жидкостей для электронных систем курения.

Для обеспечения поэтапного ограничения доступности табачных изделий, систем для потребления табака, электронных систем курения и жидкостей для них Декретом предусматривается введение запрета на использование на вывесках торговых объектов слов, тождественных или сходных с наименованием видов табачных изделий.

В Декрете также закрепляется запрет на курение в отношении вспомогательных помещений жилых домов, лифтов, автомобилей, перевозящих детей до 14 лет, детских площадок, рабочих мест в помещениях, территорий и помещений спортивно-оздоровительных лагерей, учреждений образования, подземных переходов, остановочных пунктов и посадочных площадок.

С 1 января 2020 г. введена административная ответственность за продажу табачных изделий, электронных систем курения, жидкостей для электронных систем курения, систем для потребления табака в магазинах и павильонах, имеющих торговую площадь 1000 и более кв.м, вне созданных в установленном порядке товарных отделов.

С 1 января 2022 года вводится запрет на использование для хранения и продажи табачных изделий в магазинах и павильонах оборудования, размещаемого над контрольно-кассовыми узлами.

Эти и другие глобальные и региональные инструменты в поддержку отказа от табака будут задействованы в рамках кампании Всемирного дня без табака 2021 г., один из постулатов которой заключается в том, что эффективные услуги по отказу от курения способствуют улучшению здоровья, спасению жизней и экономии средств. Каждый человек имеет право дышать воздухом, свободным от табачного дыма.