МОГИЛЁВСКИЙ ОБЛАСТНОЙ ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

ГЛАВНОЕ УПРАВЛЕНИЕ ИДЕОЛОГИЧЕСКОЙ РАБОТЫ И ПО ДЕЛАМ МОЛОДЕЖИ

ОСНОВНЫЕ АСПЕКТЫ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

материал для информационно-пропагандистских групп

г. Могилёв
май 2021 г.

ОСНОВНЫЕ АСПЕКТЫ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

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.

Справочно.

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.

Что такое киберпреступность?

Что относится к компьютерным преступлениям?

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.

Справочно.

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.

Справочно.

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.

Справочно.

Наиболее часто для совершения такого вида киберпреступлений в Беларуси в 2020 году использовалась интернет-площадка «Kufar».

Так, в 2018 году посредством нее было совершено 51 преступление, в 2019 году – 126, в первом полугодии 2020 года – 102, во втором полугодии 2020 года – 3 778.

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.

Справочно.

Зачастую при подмене оригинальных сайтов фишинговыми в именах данных ресурсов указаны наименования, созвучные с названиями банковских учреждений и сервисов: belarusbank-erip.online, ibank-belapb24.com, epey.by, e-rip.cc, erip.cc и иные. Пройдя по такому фальш-адресу и введя конфиденциальные сведения, человек отправит их непосредственно мошеннику.

2. *«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.

Справочно.

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****.*

3. *«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.

Справочно.

Упрощенно, IP-телефония – это система телефонной связи посредством сети Интернет, предоставляющая возможность осуществления звонков и голосового общения из специальных приложений с абонентами мобильных и стационарных телефонных сетей.

При таком входящем звонке жертва видит на экране мобильного телефона либо подменный номер, либо даже короткий номер банка: современные протоколы мобильной телефонии и различные компьютерные программы позволяют осуществлять

подобные телефонные звонки. Свои услуги в этом предлагают различные платные сервисы и сайты.

Для того, чтобы достоверно установить, является ли номер, с которого поступил звонок, абонентским номером телефонной сети или идентификатором IP-телефонии, необходимо направить запрос (запросы) в соответствующие телекоммуникационные организации Республики Беларусь.

Последствия использования злоумышленниками подобного способа мошенничества бывают весьма печальными.

Справочно.

Так, например, в конце марта 2021 года злоумышленник позвонил через Viber 66-летней жительнице Борисова и представился сотрудником службы безопасности банка. Он сообщил, что в целях пресечения хищения с банковской платежной карточки женщине необходимо установить определенное приложение удаленного доступа, сообщить коды карты и прислать скриншоты из мобильного банкинга, что она и сделала. Позже, заподозрив неладное, пенсионерка пошла в банк и обнаружила, что с ее карт-счета пропало почти 40 тысяч рублей.

4. *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.

5. *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.

6. *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.

7. *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.

Материал подготовлен
Академией управления при
Президенте Республики Беларусь
на основе сведений
Следственного комитета Республики Беларусь,
Министерства внутренних дел
Республики Беларусь, информационного
агентства «БелТА»

О СОСТОЯНИИ РАБОТЫ ПО ВЫЯВЛЕНИЮ ПРЕСТУПЛЕНИЙ КОРРУПЦИОННОЙ НАПРАВЛЕННОСТИ НА ТЕРРИТОРИИ МОГИЛЕВСКОЙ ОБЛАСТИ В ПЕРВОМ КВАРТАЛЕ 2021 ГОДА

Коррупция (от латинского corruptio - подкуп), комплексное явление, общепринятое толкование которого отсутствует. Термин «коррупция» можно понимать, по меньшей мере, в трех значениях в зависимости от его смысловой нагрузки - как явление социальное, уголовно-правовое и политико-экономическое.

В соответствии со статьей 1 Закона Республики Беларусь «О борьбе с коррупцией» коррупция – это умышленное использование государственным должностным или приравненным к нему лицом либо иностранным должностным лицом своего служебного положения и связанных с ним возможностей, сопряженное с противоправным получением имущества или другой выгоды в виде услуги, покровительства, обещания преимущества для себя или для третьих лиц, а равно подкуп государственного должностного или приравненного к нему лица либо иностранного должностного лица путем предоставления им имущества или другой выгоды в виде услуги, покровительства, обещания преимущества для них или для третьих лиц с тем, чтобы это государственное должностное или приравненное к нему лицо либо иностранное должностное лицо совершили действия или воздержались от их совершения при исполнении своих служебных (трудовых) обязанностей.

Конкретные проявления коррумпированности бесконечно разнообразны: от получения взяток, протекционизма (выдвижения работников по признакам родства, землячества, личной преданности, приятельских отношений) до сложных и завуалированных форм участия должностных лиц, их родственников и близких в различных сферах предпринимательской деятельности, получения незаконных доходов от деятельности субъектов хозяйствования. Коррумпированность должностных лиц высшего уровня, участвующих в законотворчестве, может проявляться в виде лоббирования за вознаграждение определенных законов, голосования определенным образом и т. д.

В уголовно-правовом значении коррупция представляет собой предусмотренные Уголовным кодексом преступления, субъектом которых являются должностные лица. Эти преступления совершаются посредством использования должностными лицами своих полномочий.

Анализируя причины и условия совершения коррупционных преступлений можно отметить, что главным фактором, мотивирующим к совершению противоправных деяний, является корысть, то есть желание должностного лица незаконно обогатиться либо получить какую-либо выгоду, а также завладеть имуществом, использовать его по своему усмотрению. Такие причины в теории называют экономическими. К данному виду причин также можно отнести:

- нестабильность в экономике, зависящая от политики и внешних влияний;

- материальная необеспеченность должностных лиц органов власти и управления, идущих на противоправные деяния ради удовлетворения собственных материальных нужд, а также нужд своей семьи;

- обеспеченность отдельных лиц, имеющих высокие доходы и свободные деньги, которые они могут использовать для подкупа должностных лиц.

Успешность борьбы с коррупцией зависит не только от планомерной и качественной работы, но и от уровня правосознания всех членов общества, желания каждого отдельного гражданина придерживаться законопослушного поведения.

Так, сотрудниками управления внутренних дел Могилевского облисполкома (далее - УВД) и территориальных органов внутренних дел (далее - ОВД) области в первом квартале 2021 года проделана определенная работа по выявлению лиц, совершивших значимые тяжкие и особо тяжкие коррупционные преступления, фактов причинения вреда в различных отраслях и сферах экономики, в первую очередь, при расходовании бюджетных денежных средств, выполнении государственных программ, осуществлении государственных закупок, а также закупок за счет собственных средств субъектами хозяйствования с долей собственности государства.

В результате проведенных мероприятий на территории Могилевской области выявлено **42** преступления коррупционной направленности в отношении **38** должностных лиц, из которых **28** относятся к категории тяжких.

Из указанного количества преступлений, **16** - связаны со взяточничеством, **19** хищений путем злоупотребления служебными полномочиями, в том числе **12** в крупном и особо крупном размерах, **6** злоупотреблений и превышений властью или служебными полномочиями.

Согласно статистическим данным, наиболее подверженными коррупционным проявлениям по-прежнему остаются сферы: промышленности **(12)**, агропромышленного комплекса **(8),** образования и ЖКХ **(по 3)**, здравоохранения и строительства **(по 2)**.

*Справочно: за указанный период учтено **18** коррупционных преступлений, по которым судами постановлены обвинительные приговоры в отношении **15** лиц, из которых **10** по ст. **210** УК (хищение путем злоупотребления служебными полномочиями); по **1** по ст. **424** УК (злоупотребление властью или служебными полномочиями, **426** УК (превышение власти или служебных полномочий) и **432** УК (посредничество во взяточничестве; **2** по ст. **430** УК (получение взятки) и **3** по ст. **431** УК (дача взятки).*

В результате проведенных мероприятий в преступной деятельности изобличено одно должностное лицо, входящее в состав депутатского корпуса.

Так, 10.02.2021 прокуратурой г. Могилева возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 210 УК (хищение путем злоупотребления служебными полномочиями), в отношении одного из руководителей государственного объединения «Жилищно-коммунальное хозяйство Могилевской области» (депутат районного совета депутатов), который в период с 01.02.2020 по 11.11.2020 давал заведомо незаконные указания подчиненным на оформление и подписание приказов о командировании работников в служебные командировки, в которые они фактически не выбывали, завладев денежными средствами объединения на сумму свыше 400 рублей.

В настоящее время наиболее подверженным коррупционным рискам является деятельность, осуществляемая субъектами хозяйствования с долей собственности государства в уставном фонде, связанная с расходованием **бюджетных денежных средств**, в том числе выделенных под **реализацию государственных программ,** осуществление **государственных закупок.**

По результатам проведенных мероприятий в данном направлении выявлено 4 коррупционных преступления, по которым в преступной деятельности изобличено 9 лиц, а установленная сумма материального ущерба составила более 240 тыс. рублей.

Так, задокументирована противоправная деятельность ведущего инженера одного из акционерных обществ г. Могилева, который действуя в сговоре с иными лицами, в период с января по февраль т.г. совершили хищение более 130 т минеральных удобрений на общую сумму более 48 000 рублей.

23, 27.02 и 16.03.2021 УСК по Могилевской области в отношении подозреваемых возбуждено три уголовных дела по признакам составов преступлений, предусмотренных ч. ч. 2-4 ст. 210 УК *(хищение путем злоупотребления служебными полномочиями).*

Изобличено во взяточничестве должностное лицо Могилевского районного потребительского общества, которое за благоприятное решение вопросов, входящих в его компетенцию, получило от представителей коммерческой структуры в качестве взятки денежные средства в размере 6 675 рублей. 27.02.2021 УСК по Могилевской области в отношении должностного лица возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 430 УК *(получение взятки)*, а в отношении представителей коммерческих структур - ч. 1 ст. 431 УК *(дача взятки).*

Проведенные мероприятия, направленные на пресечение коррупционных преступлений при осуществлении государственных закупок и закупок за счет собственных средств, позволили пресечь преступную деятельность ведущего инженера одного из строительных

предприятий и директора коммерческой структуры, которые в период с 29.04.2019 по 24.09.2019 с целью завладения денежными средствами областного бюджета организовали поставку и установку компьютерного оборудования с нарушением технических условий и характеристик, и не соответствующего требованиям проектно-сметных и аукционных документов, что повлекло причинение ущерба на общую сумму 204 190,08 рубля.

28.01.2021 прокуратурой Могилевской области в отношении последних возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 3 ст. 426 УК (*превышение власти или служебных полномочий)*.

Анализ достигнутых в отчетном периоде результатов по выявлению коррупционных преступлений свидетельствует, что по-прежнему одной из наиболее криминогенных, остается сфера **агропромышленного комплекса**.

Так, в указанной сфере за интересующий период зарегистрировано 8 преступлений с элементами коррупции, совершенных 8 должностными лицами.

Вскрыты факты коррупционных преступлений, совершенных должностными лицами АПК при производстве продукции животноводства, в частности выращивания КРС.

Так, 29.01.2021 Горецким МРОСК возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 2 ст. 424 УК *(злоупотребление властью или служебными полномочиями)*, в отношении заведующей товарной фермы сельскохозяйственной организации Горецкого района, которая в период с января по декабрь 2020 года при составлении ежемесячных отчетов о движении скота, внесла заведомо ложные сведения и записи в официальные документы, скрыв от учета падеж 52 голов молодняка КРС, и представила в бухгалтерию хозяйства подложные ведомости, подтверждающие факт получения работниками мяса выбывших на убой животных, которые на самом деле его не получали, в результате причинив существенный вред их правам и законным интересам, а из их заработной платы незаконно удержаны денежные средства в сумме 1 558 рублей.

Необходимо отметить, что в данной сфере возбуждено и 14 уголовных дел по ч. ч. 1, 2 ст. 427 *УК (не относятся к коррупционным, но также создают предпосылки для коррупции)*.

Из указанного количества выявленных преступлений 9 связаны с сокрытием падежа КРС, 1 - с приписками молока и 4 - с приписками привесов КРС и свиней.

Так, 23.03.2021 Краснопольским РОСК возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 427 УК, в отношении бригадира молочно-товарного комплекса ОАО Могилевского района, которая в мае 2020 года из корыстной заинтересованности вносила заведомо ложные сведения и записи в официальные документы, исказив показатели по надою молока на 5 000 л.

Причинами совершения должностными лицами сферы АПК преступлений, связанных с внесением заведомо ложных сведений в государственную статистическую отчетность (форма 12-сх «Отчет о состоянии животноводства»), а также ведомственную отчетность (форма 311-АПК «Отчет о движении скота и птицы на ферме»), в первую очередь, являются желание скрыть некомпетентность, недостатки и упущения в своей работе, которые приводят к сверхнормативному выбытию животных (падежу) и причинению вреда.

Основными же факторами, влияющими на непроизводственное выбытие животных, являются: ненадлежащие условия содержания скота, несоблюдение рациона его кормления, отсутствие кормов, ветеринарных препаратов и соответствующего лечения.

При этом ряд должностных лиц данные противоправные действия не только не пресекают, а напротив, злоупотребляя своими служебными полномочиями, дают незаконные указания на их совершение.

Например, 31.03.2021 прокуратурой Мстиславского района возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 427 УК, в отношении директора ОАО (депутата Мстиславского районного Совета депутатов 28 созыва), который в январе 2021 года, используя свои служебные полномочия, с целью сокрытия падежа КРС дал указание заместителю директора по животноводству, бухгалтеру по животноводству и заведующему молочно-товарного комплекса и молочно-товарной фермы, внес заведомо ложные сведения в отчеты формы 311 АПК «О движении скота и птицы».

Таким образом, причины совершения противоправных деяний в указанной сфере заключаются в стремлении должностных и иных лиц систематически получать доплаты и надбавки, избежать материальной и дисциплинарной ответственности, скрыть недостатки и упущения в своей работе, в том числе при выполнении различных показателей хозяйственной деятельности, а также желание обеспечивать комфортное пребывание в занимаемых должностях. При этом, причиняется вред, как субъекту хозяйствования, так и непосредственно работникам.

В **сфере промышленности,** за рассматриваемый период, зарегистрировано 12 коррупционных преступлений в отношении 7 лиц.

02.02.2021 прокуратурой Могилевской области возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 3 ст. 425 УК (*бездействие должностного лица)* в отношении должностного лица одного из ОАО, который, в период с 03 по 28.08.2020, умышленно из корыстной и иной личной заинтересованности, не исполнил требуемых по службе действия при наличии растущей просроченной дебиторской задолженности у ЧТУП, не приняв мер по приостановлению поставок продукции общества, причинив тем самым ущерб обществу на сумму 143 980 рублей.

12.03.2021 прокуратурой г. Могилева возбуждено уголовное дело по

признакам состава преступления, предусмотренного ч. 2 ст. 210 УК *(хищение путем злоупотребления служебными полномочиями)*, в отношении должностного лица ОАО «Могилевхимволокно», которое в июле 2019 года, путем внесения заведомо ложных сведений в бухгалтерские документы, совершил хищение товарно-материальных ценностей на сумму свыше 600 рублей.

В ходе проведенных мероприятий сотрудниками ОБЭП Осиповичского РОВД пресечена преступная деятельность должностного лица **сферы образования**, которое за благоприятное решение вопросов, входящих в его компетенцию (сдача внутреннего экзамена без надлежащей оценки знаний и получения водительского свидетельства о прохождении обучения), неоднократно получал от работников организаций и предприятий денежные средства.

11.01.2021, 01.02.2021 и 11.03.2021 Осиповичским РОСК в отношении последнего возбуждено три уголовных дела по признакам состава преступления, предусмотренного ч. 1 ст. 430 УК *(получение взятки).*

В ходе проведенных оперативно-розыскных и иных мероприятий изобличены во взяточничестве *(наиболее опасная форма коррупции)* должностные лица в сферах: промышленности, образования, здравоохранения и торговли.

Совершенные ими преступления, как правило, связаны с действиями в интересах коммерческих структур при осуществлении закупок, решением вопросов об оплате выполненных работ, поставкой продукции, выдачей разрешительных документов, сдаче экзаменов и др.

К примеру, 26.03.2021 УСК по Могилевской области возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 430 УК *(получение взятки)*, в отношении врача учреждения здравоохранения г. Могилева, который в марте т. г., за благоприятное решение вопросов, входящих в ее компетенцию (выдача справки о временной нетрудоспособности), получил в качестве взятки денежные средства.

В ходе расследования данного уголовного дела, 31.03.2021 дополнительно возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 2 ст. 430 УК.

Таким образом, коррупционные проявления характерны фактически для всех отраслей и направлений экономической деятельности, а также при выполнении должностными лицами юридически значимых действий, принятии различного рода решений, осуществлении финансово-хозяйственной деятельности.

Приведенные выше примеры совершения коррупционных преступлений свидетельствуют о необходимости принятия мер по противодействию коррупции, как со стороны правоохранительных органов, так и непосредственно самих предприятий, учреждений и организаций, и, в

первую очередь, в лице ответственных за данное направление деятельности лиц.

Кроме уголовной ответственности за совершение коррупционных преступлений, Законом Республики Беларусь от 15.07.2015 № 305-З «О борьбе с коррупцией» (далее - Закон) предусмотрен ряд антикоррупционных мер:

-установлены антикоррупционные ограничения и запреты для государственных должностных и приравненных к ним лиц;

-регламентирован порядок урегулирования конфликта интересов;

-содержится правовое регулирование декларирования доходов и имущества, устранения последствий коррупционных правонарушений, осуществления контроля и надзора за деятельностью по борьбе с коррупцией.

В первую очередь Закон направлен на внедрение профилактических механизмов, призванных минимизировать «привлекательность» совершения коррупционных деяний и исключить предпосылки для коррупционного поведения.

В частности, это запрет на трудоустройство в качестве государственных служащих работников, ранее совершивших тяжкое или особо тяжкое преступление против интересов службы либо сопряженное с использованием должностным лицом своих служебных полномочий, который не зависит от факта погашения судимости, т.е. носит бессрочный характер.

Предусмотрена норма, устанавливающая временное ограничение в приеме на руководящие должности определенных категорий лиц (в течение пяти лет со дня увольнения по дискредитирующим основаниям). Закреплен механизм лишения права на пенсионное обеспечение, предусмотренное законодательством о государственной службе.

Особое внимание уделяется соблюдению антикоррупционных ограничений. Цель таких ограничений - исключить возникновение даже видимости предрасположенности государственных должностных лиц к получению личных выгод в связи со своим служебным положением и подозрений в том, что принимаемые этими лицами решения по службе являются необъективными.

Государственное должностное лицо не вправе:

- заниматься предпринимательской деятельностью лично либо через иных лиц, оказывать содействие супругу (супруге), близким родственникам или свойственникам в осуществлении предпринимательской деятельности, используя служебное положение;

- быть представителем третьих лиц по вопросам, связанным с деятельностью государственного органа, иной организации, служащим (работником) которого (которой) оно является, либо подчиненного (подчиненной) и (или) подконтрольного (подконтрольной) ему (ей) государственного органа, иной организации;

- принимать участие лично или через иных лиц в управлении коммерческой организацией, за исключением случаев, предусмотренных настоящим Законом и иными законодательными актами;

- осуществлять поездки за счет физических и (или) юридических лиц, отношения с которыми входят в вопросы его служебной (трудовой) деятельности, за исключением служебных командировок;

- использовать во внеслужебных целях средства финансового, материально-технического и информационного обеспечения, другое имущество государственного органа, организации и информацию, распространение и (или) предоставление которой ограничено, полученные при исполнении им служебных (трудовых) обязанностей;

- выполнять иную оплачиваемую работу, не связанную с исполнением служебных (трудовых) обязанностей по месту основной службы (работы) (кроме педагогической (в части реализации содержания образовательных программ), научной, культурной, творческой деятельности и медицинской практики);

- принимать имущество (подарки), за исключением сувениров, вручаемых при проведении протокольных и иных официальных мероприятий, или получать другую выгоду для себя или для третьих лиц в виде работы, услуги в связи с исполнением служебных (трудовых) обязанностей.

Статьей 40 Закона определен порядок взыскания с государственных должностных или приравненных к ним лиц, их супруга (супруги), близких родственников или свойственников, совместно с ними проживающих и ведущих общее хозяйство, незаконно полученных денежных средств имущества, подарков, стоимости выполненных работ, оказанных услуг, которыми они незаконно воспользовались.

Кроме того, в статье 22 Закона закреплено, что государственный служащий не вправе принимать имущество (подарки) или получать другую выгоду в виде услуги, в связи с исполнением служебных обязанностей, за исключением сувениров, вручаемых при проведении протокольных и иных официальных мероприятий. При этом определено, что полученные государственными служащими при проведении протокольных и иных официальных мероприятий сувениры, стоимость которых превышает пять базовых величин, передаются в доход государства по решению комиссии, создаваемой руководителем государственного органа, в котором государственный служащий занимает государственную должность.

Материал подготовлен
УБЭП УВД Могилевского облисполкома

О ВАКЦИНАЦИИ ПРОТИВ COVID-19

Во всем мире по состоянию на 14 марта 2021 года зарегистрировано около 119,22 млн. подтвержденных случаев COVID-19, включая 2,6 млн смертей. Огромные цифры, за которыми стоят люди. Перенесенная коронавирусная инфекция даже в случае выздоровления оставляет после себя длительные последствия (так называемый постковидный синдром), что существенно влияет на качество жизни переболевших. У пациентов в течении многих месяцев могут сохраняться мышечные и головные боли, слабость, одышка, тревога и депрессия, потеря обоняния, снижение памяти и внимания, проблемы с легкими и сердцем.

Когда пандемия только началась, все страны пытались выбрать правильную и быстродейственную тактику борьбы с коронавирусом (введение ограничительных мероприятий, масочный режим, дистанционное обучение и работа и др.). Вскоре стало понятно, что только ограничительные меры не помогут справиться с пандемией, **нужен способ для формирования коллективного иммунитета** – то есть формирование большой прослойки населения, которая будет иметь иммунитет к вирусу. Коллективный иммунитет к возбудителю у населения может сформироваться **либо после перенесенного заболевания, либо после вакцинации**. Попытки достичь коллективного иммунитета, подвергая людей воздействию вируса, проблематичны с научной точки зрения и неэтичны. Тем более, что естественный иммунитет к коронавирусу (после перенесенной болезни) не пожизненный (по разным данным в среднем 3-6-9 мес.).

Несмотря на огромное число заболевших, подавляющее большинство населения в большинстве стран все же остается чувствительным к этому вирусу. Обследования распространенности по данным серологического скрининга позволяют предположить, что в большинстве стран COVID-19 инфицировано менее 10% населения. Поэтому **самый перспективный способ достижения коллективного иммунитета против COVID-19 - защита людей посредством вакцинации**.

Ожидается, что иммунитет, полученный в результате вакцинации, будет более продолжительным (при необходимости его можно будет поддерживать дополнительными дозами). Поэтому, наиболее быстрый и эффективный способ взять вирус под контроль – это вакцинация. Чем больше людей имеет иммунитет к вирусу, тем быстрее он перестанет циркулировать в человеческой популяции.

В связи с этим в мире **начата кампания вакцинация** против инфекции COVID-19 разрешенными к применению доступными вакцинами. Наша страна также присоединилась к кампании вакцинации. Это прекрасная **возможность защитить население** от коронавирусной инфекции. Такую возможность имеют далеко не все страны. Всемирная организация здравоохранения (ВОЗ) сообщает, что 60% мировых запасов вакцин от COVID-19 сейчас закупили богатые страны, население которых составляет

лишь 16% мирового населения. Это говорит о том, что вакцины достанутся не всем.

В мире более 250 вакцин против COVID-19 находится **в разработке**, 60 – проходят клинические испытания, 11 – уже используются.

По состоянию на 15 марта 2021 года в мире введено более 300 млн доз вакцины. Положительный пример - кампания вакцинаци в Израиле, который в рекордные сроки привил пять из шести миллионов взрослых граждан. Массовая вакцинация населения от COVID-19 началась в Израиле 20 декабря прошлого года. С 10 января вакцинированные начали получать вторую дозу препарата. На данный момент первая прививка сделана свыше 5,03 миллиона жителей, вторая - более 3,94 миллиона. Всего в Израиле проживает примерно 9 миллионов человек.

В Могилевской области также начата кампания вакцинации против коронавирусной инфекции.

Тактика вакцинации против COVID-19 определяется Национальным планом мероприятий по вакцинации против инфекции COVID-19 в Республике Беларусь на 2021-2022 годы, утвержденным Советом Министров Республики Беларусь от 22.02.2021г. План предполагает поэтапное проведение кампании вакцинации с обеспечением охвата не менее 60% населения каждого региона в течение за 2021год.

В первую очередь вакцинация предложена медицинским работникам, работникам учреждений с круглосуточным пребыванием детей и взрослых, а также работникам учреждений образования.

На сегодняшний день для вакцинации используется российская вакцина **Гам-КОВИД-Вак** (торговая марка **Спутник V**), разработанная Национальным исследовательским центром эпидемиологии и микробиологии имени Н.Ф. Гамалеи Минздрава **России**.

Это комбинированная **векторная вакцина** для профилактики коронавирусной инфекции, вызываемой вирусом SARS-CoV-2.

Вакцина получена биотехнологическим методом, при котором **не используется патогенный для человека коронавирус** SARS-CoV-2.

Вакцина не содержит коронавирус, вызывающий COVID-19 (ни живой, ни убитый), **поэтому заболеть из-за прививки невозможно**.

Вакцина **не содержит** адъювантов, консервантов, содержащих этилртуть.

По аналогичной технологии (с использованием аденовирусов в качестве вектора), помимо Гам-КОВИД-Вак (РФ), разрабатываются и уже используются следующие вакцины: от **Oxford – AstraZeneca** (аденовирус шимпанзе), от **Johnson & Johnson** (аденовирус 26 серотипа), от **CanSinoBIO** Пекинского института биотехнологии (аденовирус 5 серотипа).

В вакцине Спутник V используется аденовирусный вектор (2 вида аденовируса серотипов 26 и 5). Технология разработки таких вакцин – не новая и уже достаточно изученная. Вакцины на основе аденовирусных векторов изучают с 1950х годов. Несколько десятков вакцин на основе

аденовирусных векторов находятся на разных стадиях клинической разработки – это вакцины от вируса Эбола, ВИЧ, гриппа, туберкулеза и малярии. Аденовирусы сконструированы таким образом, чтобы сделать их безопасными и эффективными для использования в качестве вакцин, а также векторов для генной терапии и лечения рака. Аденовирусные векторы не способны размножаться в клетках человека.

Вакцина Спутник V прошла все необходимые **испытания безопасности и эффективности**. Данные опубликованы в авторитетном рецензируемом научном журнале The Lancet.

Результаты испытаний показывают устойчивый сильный защитный эффект во всех возрастных группах участников. **Эффективность** вакцины Гам-КОВИД-Вак против COVID-19 составила 91,6%, а против **тяжелых форм болезни – на 100%**. *Важно понимать, что не существует 100% эффективных вакцин ни от одной инфекции. Но любая вакцина существенно снижает риски заболеть, особенно в тяжелой форме, и предотвращает летальные исходы.*

Также вакцина Спутник V показала **хорошую эффективность для лиц старше 60 лет.** *По опубликованным данным 3 фазы испытаний, в исследование были включены 2144 участника старше 60 лет (1611 в группе вакцинированных и 533 в группе плацебо). Эти участники хорошо переносили вакцину, серьезных побочных эффектов не выявлено. Эффективность вакцины в этой группе участников существенно не отличалась от эффективности в возрастной группе 18–60 лет.*

Вакцина показала **хороший профиль безопасности**. Никаких серьезных нежелательных явлений, считающихся связанными с вакциной, зарегистрировано не было, что **подтверждено независимым комитетом**.

Как пройти вакцинацию?

Всем желающим сделать прививку от коронавирусной инфекции необходимо позвонить в поликлинику по месту жительства. Там вас запишут в лист ожидания и пригласят на прививку при первой возможности в порядке очереди. Записать можно себя и своих близких.

Какие противопоказания к вакцинации Спутником V?

Основное противопоказание к вакцинации Спутником V (как и к любым вакцинам) – это тяжелые аллергические реакции к какому-либо компоненту вакцины или вакцины, содержащей аналогичные компоненты, а так же тяжелые аллергические реакции в анамнезе.

Временным противопоказанием являются острые инфекционные и неинфекционные заболевания и обострение хронических заболеваний (вакцинацию проводят не ранее чем через 2-4 недели после выздоровления или ремиссии). А так же беременность, период грудного вскармливания и возраст до 18 лет.

Инструкция к вакцине не запрещает вакцинацию **лиц, которые перенесли коронавирусную инфекцию ранее,** но переболевшие COVID-19

могут отложить вакцинацию на 3-6 месяцев (независимо от тяжести течения инфекции).

Как проходит вакцинация?

Чтобы сделать прививку Гам-Ковид-вак, необходимо явиться в поликлинику дважды.

I этап. Введение первого компонента вакцины:

- **осмотр врачом-специалистом** (врач проведет общий осмотр, измерит температуру, предложит заполнить анкету о состоянии здоровья, возьмет согласие на прививку, проинформирует о возможных побочных реакциях и даст рекомендации о действиях после вакцинации);

- **вакцинация** (вакцина вводится сидя или лежа, строго внутримышечно в верхнюю треть плеча – в дельтовидную мышцу или бедро);

- **наблюдение** после процедуры в течение 30 мин (нужно оставаться в поликлинике в течение получаса после процедуры для своевременного оказания специализированной медицинской помощи в случае необходимости).

Первая доза вакцины не является защитой от инфицирования и заболевания COVID-19.

II этап. Введение второго компонента вакцины. На 21 день (без учёта дня вакцинации) необходимо повторно явиться к врачу для введения второго компонента. Процедура проходит аналогично первому этапу вакцинации.

Какие побочные реакции могут возникнуть?

Вакцины - это лекарственные средства, не быть побочных эффектов у них не может. Наоборот чем длиннее список побочных эффектов - тем лучше изучена вакцина. Риск иметь тяжелую форму заболевания выше, чем риски возникновения побочных эффектов при вакцинации.

В большинстве случаев прививка переносится хорошо, побочные эффекты не наблюдаются. Нежелательные реакции могут развиваться в первые-вторые сутки после вакцинации и разрешаются в течение 3-х последующих дней.

Чаще других могут возникнуть кратковременные общие (непродолжительный гриппоподобный синдром, характеризующийся ознобом, повышением температуры тела, артралгией, миалгией, астенией, общим недомоганием, головной болью) и местные реакции (болезненность в месте инъекции, гиперемия, отечность).

Реже отмечаются тошнота, диспепсия, снижение аппетита, иногда - увеличение регионарных лимфоузлов.

Это нормальные реакции на введение иммунобиологического препарата и не обязательно, что они возникнут у каждого и все сразу. К их возникновению просто нужно быть готовым.

Нужно ли носить маску после вакцинации и придерживаться иных мер профилактики инфекции?

Иммунитет после прививки начинает формироваться не сразу, наиболее полная защита формируется через 1-2 недели после введения второго компонента. В то же время пока нет данных, предотвращает ли вакцинация бессимптомное носительство.

Поэтому, после вакцинации против COVID-19 необходимо соблюдать все меры индивидуальной профилактики — носить маски, чаще мыть руки и соблюдать социальную дистанцию.

Такие ограничительные меры, необходимо соблюдать до тех пор, пока не будет вакцинирована значительная часть населения и пока пандемия не будет остановлена.

Материал подготовлен
УЗ «Могилевский областной центр гигиены эпидемиологии и общественного здоровья»

БЕЗОПАСНОСТЬ ЛЕТОМ

За 4 месяца текущего года в Могилевской области произошло 309 пожаров, погибло 52 человека, травмировано 18 человек.

Основными причинами возникновения возгораний стали:

- неосторожное обращение с огнём – 110 пожаров (в 2020- 116 пожаров);

-нарушение правил устройства и эксплуатации отопительного оборудования – 79 пожаров (в 2020- 81 пожар);

- нарушение правил устройства и эксплуатации электрооборудования – 62 пожара (в 2020- 50 пожаров).

- детская шалости с огнем – 1 пожар (в 2020- 3 пожара).

I.Неосторожность при курении – по-прежнему одна из основанных причин пожаров и гибели людей от них (77% из общего числа погибших). И виной тому пресловутый «человеческий фактор»: люди курят в постели, бросают окурки на пол, в качестве пепельницы используют бумажные пачки.

Пример: 2 мая около 8 часов вечера кличевские спасатели выезжали на ликвидацию возгорания частного жилого дома по ул. Набережной. Дым из-под кровли заметили соседи и позвонили по телефону 101. Дом был наполнен едким дымом. На полу без признаков жизни была обнаружена 57-летняя дочь хозяина. Поиск погибшей был затруднен высокой температурой и плотным задымлением. В результате пожара повреждено имущество в комнате, перекрытия, закопчены стены и имущество в доме. Погибшая проживала одна, не работала, со слов соседей часто коротала время в компании спиртного и сигарет. Специалисты не исключают, что в возникновении пожара виновата незатушенная сигарета.

Пример: 64-летнего жителя д. Лесные Круглянского района соседи неоднократно предупреждали, чтобы не курил в постели. Однако он, по-видимому, не прислушался к ним, что и привело к потере здоровья и жилья. Так, 22 апреля вечером пенсионер покурил перед сном, а вот окурок до конца не погасил. Около полуночи он проснулся от запаха дыма. При самостоятельной эвакуации пенсионер получил термические ожоги 23 % тела и был госпитализирован. В результате пожара уничтожена кровля, перекрытие и имущество, повреждены стены дома и сарая.

Пожары по причине неосторожного обращения с огнем связаны с халатностью и рассеянностью человека.

Пример: утром 2 апреля 83-летняя бобруйчанка поставила на газ пищу, а сама уснула. Оставленный без присмотра огонь перебросился на полотенце, лежащее около плиты и квартира стала наполняться едким дымом. Благо, пенсионерка вовремя проснулась и, вызвав спасателей, поспешила эвакуироваться. В результате пожара повреждено имущество в квартире.

Профилактика:

Не оставляйте открытый огонь (горящие свечи, газовые плиты, печи, костры) без присмотра.

Не курите в постели, гасите окурок до последней искры в пепельнице.

Не оставляйте спички и зажигалки в доступном детям месте.

Усильте контроль за Вашими престарелыми родственниками, ведь пожилые люди часто страдают потерей памяти.

II. За текущий период 2021 года в области произошло 22 пожара **автомобилей**. По статистике основными причинами автомобильных пожаров являются – короткое замыкание электропроводки и неисправности топливной системы.

Пример: 6 апреля около 9 часов утра загорелся автомобиль Мазда-6, 2003 г.в, припаркованный по ул. Рокоссовского в г. Бобруйске. В результате пожара поврежден моторный отсек, лобовое стекло и лакокрасочное покрытие капота. Причина пожара – нарушение правил эксплуатации электросетей и электрооборудования.

Пример: по аналогичной причине 6 апреля около 12 часов утра в Быхове загорелся автомобиль Ford Galaxy, 1999 г.в. Огонь повредил моторный отсек и салон автомобиля.

Пример: 9 апреля около 5 часов утра загорелся автомобиль Рено Клио, 2003 г.в., припаркованный по ул. Береговой в Бобруйске. В результате пожара поврежден моторный отсек.

В большинстве случаев горение в автомобиле начинается под капотом. Если Вы почувствовали резкий запах бензина, горелой резины: осторожно откройте капот – желательно сбоку палкой или монтировкой, помните, что при открытии возможен выброс пламени. Направьте огнетушитель на очаг наиболее интенсивного горения или накройте пламя брезентом, забросайте песком, рыхлой землей, залейте водой. Не приступайте к тушению, если вы в промасленной одежде или ваши руки смочены бензином. Если Вы чувствуете, что самостоятельно справиться с огнем не получится – не геройствуйте, вызывайте спасателей по телефонам 101 или 112.

III. Для того, чтобы обезопасить свое жилье от пожара, помимо строгого соблюдения правил безопасности, в каждой жилой комнате необходимо установить автономный пожарный извещатель (далее АПИ).

Пример: ангелом-хранителем для многодетной семьи из Осипович стал автономный пожарный извещатель. Так, 6 мая около 6 часов утра шестилетнего Никиту, проживающего с родителями и четырьмя малолетними братьями и сестрами (2013, 2016, 2017 и 2020 г.р.) в двухкомнатной квартире девятиэтажного жилого дома по пер. Черняховского, разбудил звук сработавшего автономного пожарного извещателя. Мальчик разбудил родителей, и семья незамедлительно покинула квартиру. Эвакуация понадобилась и двоим жильцам вышележащих этажей. В результате пожара повреждено имущество в комнате, закопчены стены и потолок в квартире. Причина пожара устанавливается.

Страшно представить последствия этого пожара, если бы в квартире отсутствовал автономный пожарный извещатель. Ведь когда человек спит -

он не чувствует запах дыма и легко становится жертвой огня. В текущем году благодаря АПИ в Республике спасено 39 человек, в том числе 9 детей. В Могилевской области на счету спасения АПИ - 13 человек, в том числе 5 детей.

Очень важно верно выбрать место установки извещателя. Оптимальная точка – в центральной части потолка с небольшим смещением в сторону окна или двери, где происходит движение воздушных потоков. Многих интересует, как прекратить звучание, если АПИ сработал не от пожара. Для этого необходимо проветрить помещение либо в течение нескольких секунд пропылесосить АПИ, не снимая с потолка.

В процессе эксплуатации АПИ необходимо осуществлять его техническое обслуживание, которое заключается в очистке оптической системы извещателя при помощи фена в холодном режиме на максимальной мощности. Не разбирая извещатель, струю воздуха направьте на защитную сетку оптического элемента. Периодичность чистки не реже одного раза в год и при каждой ложной сработке. Также необходимо регулярно менять элемент питания – «крону». О том, что пришло время это делать, извещатель сообщит постоянной подачей короткого звукового сигнала. Не экономьте на безопасности – жизнь и здоровье дороже!

IV.С приходом теплой погоды значительно возрастает количество ЧС с участием детей и подростков: выпал из окна, упал в колодец, засыпало в карьере, делал селфи в опасном месте, погиб на пожаре, получил поражение электрическим током.

Пример: 22 апреля днем 16-летний подросток рыбачил на озере возле деревни Гуторовщина Мстиславского района. При забросе снасти он удочкой коснулся проводов ЛЭП — и получил удар электрическим током. От электрического разряда на парне загорелась одежда. Рыбаки, которые находились рядом, вызвали скорую и оказали ему помощь. Подросток получил ожоги более 70% тела. Из центральной районной больницы санитарной авиацией МЧС его транспортировали в Республиканский ожоговый центр. Сейчас за его жизнь борются врачи.

Не смотря на неоднократные предупреждения об опасности нахождения людей вблизи высоковольтных линий электропередач, ежегодно происходят несчастные случаи, связанные с поражением электрическим током во время рыбалки или отдыха.

Находясь на рыбной ловле, категорически запрещается ловить рыбу в охранной зоне ЛЭП – ближе 10 метров от крайнего провода. На водоеме достаточно других мест, чтобы организовать рыбалку или отдых. Будьте внимательны и при перемещениях вдоль реки под проводами линий. Необходимо предварительно складывать удилища во избежание случайного прикосновения к проводам.

Современные удилища длинной от 7 метров и выше изготавливаются из углепластика, материала, который является проводником электрического тока. Повышенная влажность в границах водоема, мокрая леска и удилище

создают угрозу жизни даже при приближении к проводам действующей линии электропередачи, а касание к проводам неизбежно приведет к летальному исходу. Предупредите об этом своих детей, даже если Вам кажется, что они уже достаточно взрослые и самостоятельные.

Пример: днем 17 апреля 17-летний парень находился на территории незавершенного строительства больницы в Осиповичах. Он нанес несколько ударов ногой по кирпичной стене, в результате чего произошло обрушение трех железобетонных плит перекрытия на втором этаже указанного здания. При падении одна из плит придавила подростка. На данном недостроенном объекте постоянно играют дети. Двое мальчиков увидели произошедшее и позвали на помощь. С тяжкими телесными повреждениями пострадавший был госпитализирован. В настоящий момент его жизни ничего не угрожает. Предполагаемая причина обрушения — ветхость несущих конструкций здания.

Здание, в котором произошло обрушение железобетонной плиты, представляет собой объект незавершенного строительства, к которому собственником не ограничен свободный доступ посторонних лиц.

Игры – любимые занятия детей. Однако нужно помнить, что игры бывают разные: подвижные, спокойные и опасные. К последним относятся игры в заброшенных домах, на чердаках, стройках, железнодорожных переездах, карьерах, вблизи трассы и водоемов. Эти места представляют наибольшую опасность для жизни и здоровья. Чтобы с Вашими детьми не случилось беды, постарайтесь организовать им безопасный досуг. Постоянно отслеживайте местонахождение ребенка. Поговорите, предостерегите, убедите, тем самым Вы оградите их от беды.

V.С целью привлечения внимания к проблеме детской шалости с огнем и гибели детей на пожарах, снижения количества чрезвычайных ситуаций с участием детей и обеспечения их общей безопасности с **3 мая** в области стартовала республиканская профилактическая акция **«Не оставляйте детей одних!»**, приуроченная к Международному Дню семьи и Дню защиты детей.

Акция состоит из 4 этапов:

1-й этап: с 3 по 15 мая. Целевая аудитория данного этапа – родители и их дети. Акция проводилась на объектах с массовым пребыванием людей (торгово-развлекательные центры, кинотеатры, детские театры, в детских магазинах «Буслик», «Kari kids», на открытых площадках и др.). Желающие принимали участие в семейном спортивном празднике «Мама, папа, мы – в безопасности сильны!».

2-й этап: 17-21 мая – проводится в учреждениях здравоохранения (территориальные поликлиники): «Кабинеты здорового ребенка», «Школы материнства»;

- в учреждениях образования (школы раннего развития, центры дошкольного образования); Центрах внешкольного образования (Дворцы детей и молодежи); в физкультурно-оздоровительных комплексах, спортивных школах (комнаты ожидания для родителей);

- в дошкольных учреждениях, начальных классах общеобразовательных учреждений (родительские собрания). Целевая аудитория этапа – будущие и молодые мамы, родители.

3-й этап: 24 мая – 28 мая - спасатели с развлекательно-профилактической миссией посетят многодетные семьи, детские дома семейного типа, детские развлекательные центры, организации общественного питания. В районных центрах мероприятия будут проходить в районных Домах культуры.

4-й этап: с 31 мая по 1 июня. Приурочен к Международному Дню защиты детей. Акция пройдет на открытых площадках в местах с массовым пребыванием людей.

Пусть детство будет безопасным!!!!

Материал подготовлен
Могилевский областным
УМЧС Республики Беларусь